

Estudo Técnico Preliminar 56/2025

1. Informações Básicas

Número do processo: 60596.000023/2024-79

2. Descrição da necessidade

Problema Identificado: A Segurança na Tecnologia da Informação tem se tornado um desafio crescente devido ao aumento constante de ameaças cibernéticas, como ataques de hackers, e-mails maliciosos, roubo de informações sensíveis e outras formas de intrusão. A falta de medidas de segurança robustas deixa as redes e sistemas vulneráveis a essas ameaças, resultando em possíveis perdas financeiras, danos à reputação e comprometimento de dados sensíveis.

Necessidade: Proteger a infraestrutura da rede da Administração Central do Ministério da Defesa (ACMD), utilizada por todo Ministério da Defesa (MD), e da Rede Operacional de Defesa (ROD), utilizada pelo Estado-Maior Conjunto das Forças Armadas (EMCFA), contra ameaças cibernéticas, garantindo a segurança dos dados e a continuidade dos serviços. Para tanto, faz-se necessário analisar as necessidades de soluções de Tecnologia da Informação e Comunicação (TIC), com vistas ao desenvolvimento ou à contratação de tais soluções.

2.1 - Motivação/Justificativa

2.1.1 - Área de negócio: Secretaria Geral

Compete à Coordenação de Segurança Cibernética (COSEC), do Departamento de Tecnologia da Informação e Comunicação (DETIC), planejar, implantar, administrar e manter os ativos de Segurança de TIC no âmbito da administração central do Ministério da Defesa.

Atualmente, a COSEC mantém em funcionamento diversas ferramentas e soluções de segurança de TIC, que englobam equipamentos (hardwares) e sistemas (softwares), e que, trabalhando em conjunto, garantem níveis de segurança aceitáveis aos usuários da rede administrativa da ACMD no desenvolvimento de suas atividades laborais.

As ferramentas e os equipamentos de segurança, responsáveis atualmente pelas proteções aos usuários da rede administrativa da ACMD, estão suportados por contratos em fase final de vigência, em **29/09/2025**, e, portanto, faz-se necessária uma nova contratação que permita garantir a manutenção da segurança de TI da referida rede ACMD. Além disso, é essencial adquirir novas ferramentas para ampliar essa segurança, em conformidade com os normativos vigentes, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD) e para cumprir as determinações constantes do Programa de Privacidade e Segurança da Informação (PPSI).

Nesse sentido, para a continuidade e modernização das soluções de segurança existentes, são relacionadas as seguintes necessidades de negócio a serem atendidas:

- a) Necessidade de proteção das Estações de Trabalho (ET);
- b) Necessidade de monitoramento e a proteção do sistema de arquivos e dos bancos de dados;
- c) Necessidade de proteção e o controle da Internet disponibilizada aos usuários;
- d) Necessidade de proteção do trâmite de mensagens do Correio Eletrônico corporativo;
- e) Necessidade de proteção do Sistema Eletrônico de Informações (SEI);
- f) Necessidade de proteção das redes internas;
- g) Necessidade de proteção da rede sem fio;
- h) Necessidade de proteção dos portais (defesa.gov.br);
- i) Necessidade de proteção dos sistemas corporativos;
- j) Necessidade de realizar varreduras de vulnerabilidades;
- k) Necessidade de detecção e impedimento de acesso privilegiado não autorizado a recursos críticos; e
- l) Necessidade de realizar auditorias e verificações de conformidade.

2.1.2 - Área de negócio: EMCFA

Compete à SC-1.3 (Seção Técnica de Comando e Controle) juntamente com a SC-1.1 (Seção de Defesa Cibernética e Guerra Eletrônica), da SC-1 (Subchefia de Comando e Controle), planejar, implantar, administrar e manter os ativos de Segurança de TIC no âmbito do EMCFA do Ministério da Defesa.

Atualmente, a SC-1 mantém em funcionamento diversas ferramentas e soluções de segurança de TIC, que englobam equipamentos (hardware) e sistemas (software), e que, trabalhando em conjunto, garantem níveis de segurança aceitáveis aos diversos usuários da ROD no desempenho de suas atividades laborais.

As ferramentas e os equipamentos de segurança, responsáveis atualmente pelas proteções aos usuários da ROD, estão suportados por contratos que com encerramento de vigência previsto para **29/09/2025** e, portanto, faz-se necessária uma nova contratação que permita garantir a manutenção da segurança de TI da referida ROD. Além disso, as novas ameaças cibernéticas tornam essencial a aquisição de novas ferramentas para ampliar o nível de segurança da rede, em conformidade com os normativos vigentes, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD) e para cumprir as determinações constantes do Programa de Privacidade e Segurança da Informação (PPSI).

Nesse sentido, para a continuidade e modernização das soluções de segurança existentes, são relacionadas as seguintes necessidades de negócio a serem atendidas:

- a) Necessidade de proteção das Estações de Trabalho (ET);
- b) Necessidade de monitoramento e a proteção do sistema de arquivos e dos bancos de dados utilizados pelos sistemas;
- c) Necessidade de proteção e o controle nos acessos à Internet disponibilizada aos usuários;
- d) Necessidade de proteção das redes internas;
- e) Necessidade de proteção dos sistemas corporativos; e
- f) Necessidade de realizar auditorias e verificações de conformidade.

2.1.3 - Alinhamento com o Plano Estratégico Organizacional do Ministério da Defesa –

PEO-MD 2024-2027

Objetivo Estratégico 12: Aperfeiçoar a infraestrutura física e tecnológica.

Aperfeiçoar a infraestrutura física e tecnológica, em especial de tecnologia da informação, colocada à disposição das unidades do Ministério, observando as

necessidades, de forma a facilitar o trabalho, propiciar o bom desempenho e garantir a saúde e o bem-estar no ambiente de trabalho.

2.1.4 - Alinhamento com o Plano Diretor de Tecnologia da Informação PDTI – MD 2024-2027

NL15: Licença de uso de software/programa para equipamento de detecção e prevenção de intrusão de rede do tipo IDS/IPS;

NL16: Licença de uso de software/programa para equipamento de segurança de rede do tipo Firewall;

NL18: Licença de uso de software/programa de proteção de endpoints do tipo Antimalware e EDR;

NL19: Licença de uso de software/programa de prevenção de perda de dados do tipo DLP;

NL20: Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway;

NL21: Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure Email Gateway;

NL22: Licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades; e

NL23: Licença de uso de software/programa de segurança de identidades do tipo PAM (Privileged Access Management).

2.1.5 - Alinhamento com o Plano de Contratações Anual (PCA)

A contratação pleiteada está prevista no PCA: DFD - 296/2024 Solução de segurança cibernética.

3. Área requisitante

Área Requisitante	Responsável
Coordenadoria de Segurança Cibernética (COSEC) – Subordinado ao Departamento de Tecnologia da Informação e Comunicação (DETIC) do Ministério da Defesa	Capitão de Fragata (T) Fernando Nogueira Filho – 010.479.957-94 – Assistente Militar
Subchefia de Comando e Controle (SC-1) – Subordinada à Chefia de Operações Conjuntas (CHOC) do Estado Maior Conjunto das Forças Armadas (EMCFA) do Ministério da Defesa	Coronel Junier Caminha Amorim – 690.250.961-15 – Adjunto da Seção Técnica (SC-1.3)

4. Necessidades de Negócio

4.1 - Área de negócio: Secretaria Geral

4.1.1 - Garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados e informações na rede da ACMD - A rede de dados da ACMD lida diariamente com uma grande diversidade de informações. Portanto, é essencial que as equipes da DETIC preservem a **confidencialidade** (garantindo que informações sensíveis sejam acessíveis apenas por pessoas autorizadas), a **integridade** (assegurando que as informações não sejam alteradas de maneira não autorizada), a **disponibilidade** (garantindo que as informações estejam disponíveis quando necessário) dessas informações e a **autenticidade** (garantindo que as informações ou transações são genuínas e provêm de uma fonte confiável).

4.1.2 - Utilizar ferramentas de software na proteção aos sistemas, dados e informações da ACMD - Sendo assim, faz-se necessário o uso de ferramentas de segurança para administrar e proteger as atividades do negócio do Ministério da Defesa. Essas ferramentas de segurança são fundamentais para a manutenção da proteção cibernética da rede, oferecendo segurança 24 horas por dia, 7 dias por semana. Isso inclui a proteção de todos os ativos físicos da rede (servidores, dispositivos de conectividade, computadores, notebooks e dispositivos móveis) e das informações contidas nesses equipamentos (sistemas operacionais, aplicativos, páginas da internet e bancos de dados) contra ataques internos e externos.

4.1.3 - Manter a segurança da informação, no serviço público, no que tange ao Ministério da defesa, contra ataques digitais - A preocupação com a cibersegurança no setor público tem crescido significativamente nos últimos anos, refletindo a importância da proteção das informações. Entidades governamentais em todo o mundo têm sofrido diversos ataques digitais, incluindo negação de serviço, roubo de informações, alterações de páginas e dados, e ataques direcionados e persistentes. Esses eventos resultam em retrabalho significativo para a recuperação das informações, prejuízos

financeiros e danos à imagem pública, levando os órgãos públicos a reforçarem seus níveis de proteção da rede.

4.1.4 - Modernizar os ativos de segurança cibernética - Nesse contexto, para proteger os ativos físicos da rede e as informações, é necessário que os órgãos públicos invistam cada vez mais em mecanismos eficazes e eficientes de proteção contra crimes cibernéticos, destacando-se as modernas soluções de ferramentas de segurança.

4.1.5 – Preservar e ampliar o nível de proteção cibernética provido pelo atual contrato existente - A rede ACMD possui diversas ferramentas de segurança que oferecem múltiplas camadas de proteção. No entanto, essas ferramentas precisam de licenciamento para operar. Atualmente, essas licenças têm como data de término da vigência do suporte técnico o dia **29/09/2025**. Além disso, novas ferramentas de segurança são necessárias para ampliar o nível de segurança da rede devido à constante evolução dos atacantes.

4.1.6 – Em virtude do exposto, identificou-se a necessidade de contratar licenças para as ferramentas de segurança atualmente em uso e para novas ferramentas, visando garantir a proteção contínua da rede ACMD.

4.2 - Área de negócio: EMCFA

4.2.1 - Garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados e informações na rede da ROD - A ROD é a infraestrutura de conectividade empregada pelo EMCFA nas Operações Conjuntas e, pela natureza de tais atividades, lida com dados sensíveis e que precisam ser garantidos pelas ferramentas de tecnologia empregadas. Portanto, é essencial que as equipes da SC-1 preservem a **confidencialidade** (garantindo que informações sensíveis sejam acessíveis apenas por pessoas autorizadas), a **integridade** (assegurando que as informações não sejam alteradas de maneira não autorizada), a **disponibilidade** (garantindo que as informações estejam disponíveis quando necessário) e a **autenticidade** (garantindo que as informações ou transações são genuínas e provêm de uma fonte confiável) dessas informações.

4.2.2 – Utilizar ferramentas de software na proteção aos sistemas, dados e informações da ROD - Sendo assim, faz-se necessário o uso combinado de ferramentas de segurança para administrar e proteger os dados gerados e transmitidos pelo EMCFA em suas atividades operativas. Essas ferramentas de segurança são fundamentais para a manutenção da proteção cibernética da rede, oferecendo

segurança 24 horas por dia, 7 dias por semana. Isso inclui a proteção de todos os ativos físicos da rede (servidores, dispositivos de conectividade, computadores, notebooks e dispositivos móveis) e das informações contidas nesses equipamentos (sistemas operacionais, aplicativos, páginas da internet e bancos de dados) contra ataques internos e externos.

4.2.3 - Manter a segurança da informação, no serviço público, no que tange ao Ministério da defesa, contra ataques digitais - A preocupação com a cibersegurança no setor público tem crescido significativamente nos últimos anos, refletindo a importância da proteção das informações. Entidades governamentais em todo o mundo têm sofrido diversos ataques digitais, incluindo negação de serviço, roubo de informações, alterações de páginas e dados, e ataques direcionados e persistentes. Esses eventos resultam em retrabalho significativo para a recuperação das informações, prejuízos financeiros e danos à imagem pública, levando os órgãos públicos a reforçarem seus níveis de proteção da rede.

4.2.4 - Modernizar os ativos de segurança cibernética - Nesse contexto, agravado pela natureza das informações trafegadas na ROD, para prover a devida proteção na rede, é necessário que EMCFA realize investimentos na aquisição de soluções cada vez mais eficazes e eficientes de proteção contra crimes cibernéticos.

4.2.5 – Preservar e ampliar o nível de proteção cibernética provido pelo atual contrato existente - A ROD possui, atualmente, algumas ferramentas de segurança que oferecem múltiplas camadas de proteção. No entanto, essas ferramentas precisam de licenciamento para operar. Tais licenças têm como data de término da vigência do suporte técnico o dia **29/09/2025**. Além disso, novas ferramentas de segurança são necessárias para ampliar o nível de segurança da rede devido à constante evolução dos atacantes e atender áreas que ainda estão descobertas na rede.

4.2.6 – Em virtude do exposto, identificou-se a necessidade de realizar a contratação de soluções de segurança cibernética que englobem tanto a continuidade das atuais ferramentas utilizadas, bem como a aquisição de novas soluções para cobrir as demandas de segurança resultantes das novas ameaças. Tais soluções poderão ser compostas apenas por licenças de software ou com a combinação de hardware (*appliance*) de acordo com os estudos apresentados pelo presente documento.

5. Necessidades Tecnológicas

A DETIC e o EMCFA necessitam contratar as seguintes soluções para manter a atual estrutura de segurança, ou ampliando-a com novas ferramentas para aprimorar a proteção, conforme descrito a seguir:

5.1 – Necessidade de aquisição de licença de uso de software/programa de proteção de endpoints (dispositivos de usuário final e servidores) do tipo Antimalware e EDR (Endpoint Detection and Response - Detecção e Resposta de Estação de Trabalho), com instalação, configuração, suporte técnico e repasse de conhecimento.

A Política de Segurança da Informação da administração central do Ministério da Defesa (POSIN-MD), Portaria GM-MD Nº 5.659, 18 de novembro de 2022, no seu item 4.3.3 informa que os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de reduzir ameaças e minimizar riscos às atividades e aos objetivos de negócio da ACMD. Desta forma, é de extrema importância proteger os *endpoints* de ataques cibernéticos, como vírus, ransomware, spyware e outros tipos de malware. Um antimalware eficaz pode detectar e neutralizar essas ameaças antes que causem danos significativos a estrutura das redes administradas no MD. A ferramenta EDR serve para monitorar continuamente os endpoints em tempo real, identificando comportamentos suspeitos e ameaças avançadas, sendo extremamente importante para complementar a proteção dos endpoints, juntamente com o antimalware, proporcionando uma defesa mais robusta e eficaz contra-ataques cibernéticos.

5.1.1 - A aquisição de uma solução de EDR representa uma evolução funcional necessária em relação à solução anterior, diante do atual cenário de ameaças cibernéticas, que demanda mecanismos mais sofisticados de proteção, detecção e resposta em endpoints. Diferentemente da solução apenas de Antimalware, o EDR oferece visibilidade contínua e em tempo real sobre as atividades dos dispositivos da rede, permitindo o monitoramento detalhado de processos, conexões e comportamentos suspeitos. Por meio de análise comportamental avançada, o EDR identifica padrões anômalos que podem indicar ameaças como malwares, ataques direcionados ou movimentações laterais, funcionalidades que não estavam previstas na licitação anterior. A inclusão dessa tecnologia visa fortalecer a postura de segurança cibernética do Ministério da Defesa, alinhando-se às melhores práticas do setor e às exigências atuais de proteção de ativos críticos.

5.2 – Necessidade de aquisição de licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.

A Norma Complementar Nº 03 do MD, no seu item 8.1, alínea b, informa que o Ministério da Defesa deverá disponibilizar soluções de segurança tais como: firewall, serviço de autenticação, Proxy e servidor de log. O proxy é uma ferramenta importante na proteção da rede contra ameaças externas, como vírus e ataques cibernéticos, ao filtrar o tráfego de internet e bloquear sites maliciosos, por meio da definição de regras específicas sobre quem pode acessar determinados sites e serviços, em quais horários

e com qual consumo de internet. Essa filtragem é realizada por meio do direcionamento de todo o tráfego de rede para o PROXY, que fica responsável por encaminhar para a internet. Isso é essencial para manter a produtividade e evitar o uso indevido da rede e por fim, registra (auditoria) de todas as atividades de navegação, permitindo o monitoramento do uso da internet e a identificação de usuários com comportamentos inadequados ou suspeitos.

5.3 - Necessidade de aquisição de licença de uso de software/programa de prevenção de perda de dados do tipo DLP (*Data Loss Prevention* - Prevenção contra Perda de Dados), com instalação, configuração, suporte técnico e repasse de conhecimento.

No item 4.3.1 da POSIN-MD, é definido que toda informação tratada por usuário, no exercício de suas atividades, é considerada bem e propriedade do MD e deve ser protegida segundo as diretrizes descritas na referida norma e demais regulamentações em vigor. O software DLP ajuda a identificar, monitorar e proteger dados reservados contra acessos não autorizados e vazamentos por pessoas internas da organização, garantindo a integridade e a confidencialidade das informações. O uso de DLP ajuda a garantir também que a instituição esteja em conformidade com a LGPD (Lei Geral de Proteção de Dados).

5.4 - Necessidade de aquisição de solução de prevenção e detecção de intrusão de rede do tipo IPS (*Intrusion Prevention System* - Sistema de Prevenção de Intrusões), com instalação, configuração, suporte técnico e repasse de conhecimento.

No item 4.3.3 da POSIN-MD, é definido que os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de reduzir ameaças e minimizar riscos às atividades e aos objetivos de negócio da ACMD e no item 4.9.1 da mesma norma, informa que o controle de acesso aos ativos de informação e às áreas e instalações deve ser implantado nos níveis físico e lógico, conforme procedimentos estabelecidos pelas áreas competentes.

Sendo assim, a necessidade de uma ferramenta como o IPS que possui como principal finalidade monitorar o tráfego de rede em tempo real, podendo detectar e bloquear atividades maliciosas, como tentativas de invasão, ataques de negação de serviço (DDoS) e exploração de vulnerabilidades. Diferente de sistemas de detecção de intrusões (IDS), que apenas alertam sobre possíveis ameaças, o IPS pode tomar medidas imediatas para prevenir ataques, aumentando a segurança da rede DETIC (ACMD) e do EMCFA (ROD).

5.5 - Necessidade de aquisição de licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure E-Mail Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.

A Norma Complementar Nº 04 do MD, no seu item 4.4.1, alínea f, informa que se deve manter proteção contra vírus, mensagens não solicitadas (Spam), Phishing, material obsceno, pornográfico, ofensivo, preconceituoso ou de qualquer forma contrário à lei e aos bons costumes nos servidores do correio eletrônico. E-mails maliciosos frequentemente contêm anexos ou links que, quando abertos, instalam malware no sistema. Esse malware pode roubar dados, danificar arquivos, criptografar dados ou permitir acesso não autorizado à rede de computadores. A solução de Antispam ajuda a bloquear e-mails maliciosos que podem conter vírus, malwares, Phishing e outras ameaças cibernéticas.

5.6 - Necessidade de aquisição de licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades, com instalação, configuração, suporte técnico e repasse de conhecimento.

No item 4.6.1 da POSIN-MD, informa que o risco de segurança da informação está associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, devendo ser continuamente monitorado e tratado, conforme legislação em vigor. A ferramenta de verificação de vulnerabilidades ajuda a identificar e corrigir falhas de segurança antes que sejam exploradas por cibercriminosos. Isso inclui vulnerabilidades em sistemas operacionais, aplicativos, sistemas Web e servidores e dispositivos de rede. Ao identificar e corrigir vulnerabilidades, a organização pode prevenir ataques cibernéticos que poderiam resultar em perda de dados, interrupção de serviços e danos à reputação.

5.7 - Necessidade de aquisição de solução de proteção de segurança de rede do tipo Firewall, com instalação, configuração, suporte técnico e repasse de conhecimento.

Semelhante ao subitem 5.4 deste ETP, é necessário também referenciar os itens 4.3.3 e 4.9.1 da POSIN-MD para a proteção e segurança da rede utilizando a ferramenta de segurança Firewall. O firewall atua como uma barreira entre a rede interna e externa, bloqueando tentativas de acesso não autorizadas e prevenindo invasões. Além disso, ele permite monitorar e controlar o tráfego de dados que entra e sai da rede, garantindo que apenas informações seguras e autorizadas circulem. O firewall também oferece proteção contra uma variedade de ataques cibernéticos, incluindo malware, ransomware e ataques de negação de serviço (DDoS).

5.8 - Necessidade de aquisição de licença de uso de software/programa de detecção e impedimento de acesso privilegiado não autorizado a recursos críticos do tipo PAM (Privileged Access Management – Gerenciamento de Acesso Privilegiado), com instalação, configuração, suporte técnico e repasse de conhecimento.

A aquisição de uma ferramenta de PAM é importantíssimo para fortalecer a segurança da informação na ACMD. As contas privilegiadas (exemplo: conta Administrador) são frequentemente alvos de ataques cibernéticos devido ao seu alto nível de acesso. A ferramenta PAM ajuda a proteger essas credenciais, armazenando-as em um repositório seguro e controlando o acesso a elas. Além disso, a referida ferramenta monitora e registra todas as atividades relacionadas a contas privilegiadas, permitindo a detecção e resposta rápida a atividades suspeitas, prevenindo tanto ameaças internas quanto externas, bem como, auxiliando em auditorias no caso de mau uso da conta privilegiada.

Observação: As definições detalhadas dos requisitos técnicos, de cada necessidade, estão descritas no Anexo I do presente documento.

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

6.1 - Para cada uma das necessidades tecnológicas elencadas, são necessárias a previsão de instalação, configuração, manutenção (preventiva, corretiva e evolutiva), de suporte técnico, e de repasse de conhecimento.

6.2 - Para a manutenção dos níveis de segurança já implementados nas redes de dados da ACMD, as soluções a serem adquiridas e implementadas devem ter a sua capacidade e efetividade **iguais ou superiores às atuais**, ou seja, os requisitos técnicos serão baseados nas soluções que estão atualmente em funcionamento.

6.3 – As soluções de proteção de endpoints do tipo Antimalware/EDR, filtragem e proteção de navegação Web do tipo Secure Web Gateway, prevenção de perda de dados do tipo DLP e de prevenção e detecção de intrusão de rede do tipo IPS devem possuir o nível de integração que permita:

- A completa compatibilidade entre as soluções;
- A interoperabilidade de indicadores de comprometimento entre todas as soluções;
- A capacidade de retroalimentação automatizada de dados de inteligência e reputação, onde um artefato ou endereço malicioso possa ser compartilhado entre as soluções;
- A capacidade de operação e contenção integradas; e
- A capacidade de manutenção do nível funcional de investigação e resposta, hoje existentes com a topologia atual.

Desta forma, permite uma postura de segurança coesa e eficiente por meio da integração robusta dessas soluções, oferecendo centralização e controle completo sobre o ambiente de TI, facilitando a gestão e otimizando a resposta a incidentes.

Além dos ganhos da integração robusta dessas ferramentas, observa-se um ganho de produtividade com resultados consistentes e a redução significativa dos custos operacionais inerentes à administração de múltiplas plataformas, tendo em vista que:

- A centralização das soluções em uma plataforma unificada elimina a necessidade de ferramentas de terceiros, simplificando a infraestrutura de TI e reduzindo os custos com licenciamento e treinamento; e
- A integração entre as soluções viabiliza a identificação e a resposta mais ágil a incidentes de segurança, mitigando a probabilidade de impactos financeiros, danos à reputação institucional ou comprometimento de dados sensíveis.

6.4 - Para a manutenção da disponibilidade dos serviços de Internet, do envio e recebimento de e-mails e das proteções das redes da ACMD, as soluções de número 5.2 (Filtragem e proteção de navegação Web do tipo Secure Web Gateway), 5.4 (Detecção e prevenção de intrusão de rede do tipo IPS), 5.5 (Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway), 5.7 (Segurança de rede do tipo Firewall) devem ser implementadas de forma redundante, com equipamentos/sistemas a serem instalados em centros de processamento de dados distintos.

6.5 - As equipes técnicas da COSEC e da SC-1 deverão ser capacitadas para operar todas as soluções tecnológicas como forma de garantir a devida independência tecnológica com relação ao fornecedor da solução.

6.6 - O repasse de conhecimento deverá ser realizado pela contratada durante os trabalhos de instalação, configuração e manutenção das soluções adquiridas, de modo a capacitar as equipes técnicas do MD para operar e configurar as ferramentas diante de demandas internas imediatas, conferindo um nível adequado de autonomia.

6.7 - Ao adquirir-se as soluções pretendidas, busca-se o melhor atendimento às necessidades do órgão com a melhor eficiência possível, portanto, para as atividades de manutenção e suporte técnico serão permitidos, quando possível, o atendimento na modalidade remota.

6.8 - Todas as soluções deverão ser instaladas e configuradas, pela(s) contratada(s), nos centros de processamento de dados do MD ou nos locais indicados pela equipe da COSEC e da SC-1.

6.9 - As soluções a serem adquiridas devem permitir a instalação em ambientes tecnológicos distintos, uma vez que serão utilizadas em redes segregadas e operadas de forma independente pelas equipes da COSEC e da SC-1.

6.10 - A solução 5.4 é descrita como "Aquisição de solução de prevenção e detecção de intrusão de rede do tipo IPS" devido à presença de 02 (dois) equipamentos atualmente em uso na rede ACMD e à necessidade de aquisição de 02 (dois) equipamentos para a rede ROD, que atualmente não possui essa solução.

6.10.1 – Para a rede ACMD, considerando que já existem dois equipamentos IPS da marca McAfee, modelo IPS-NS7500, em funcionamento, a solução de prevenção e detecção de intrusão de rede do tipo IPS pode ser composta apenas pela licença de uso de software/programa de modo a habilitar todos os recursos dos equipamentos ou com o conjunto completo de licença de uso de software/programa e equipamentos, desde que atendendo aos requisitos da especificação técnica do Anexo I deste ETP.

6.10.2 – Para a rede ROD, devido à inexistência de equipamentos IPS em funcionamento, a solução de prevenção e detecção de intrusão de rede do tipo IPS deve ser adquirida como um conjunto completo de licença de uso de software /programa e equipamento, atendendo aos requisitos da especificação técnica do Anexo I deste ETP.

6.11 - A solução 5.7 é descrita como "Aquisição de solução de proteção de segurança de rede do tipo Firewall" devido à presença de 04 (quatro) equipamentos atualmente em uso na rede ACMD e à presença de 03 (três) equipamentos para a rede ROD.

6.11.1 – Para a rede ACMD, considerando que já existem quatro equipamentos Firewall da marca Palo Alto, fabricante Palo Alto, modelo/versão PA3410, em funcionamento, a solução de proteção de segurança de rede do tipo Firewall pode ser adquirida apenas com a licença de uso de software/programa ou com o conjunto completo de licença de uso de software/programa e equipamento, desde que atendendo aos requisitos da especificação técnica do Anexo I deste ETP.

6.11.2 – Para a rede ROD, considerando que já existem três equipamentos Firewall da marca Palo Alto, fabricante Palo Alto, modelo/versão PA850, em funcionamento, a

solução de proteção de segurança de rede do tipo Firewall pode ser adquirida apenas com a licença de uso de software/programa ou com o conjunto completo de licença de uso de software/programa e equipamento, desde que atendendo aos requisitos da especificação técnica do Anexo I deste ETP.

6.12 - Em conformidade com o acórdão do Tribunal de Contas da União (TCU) nº 2265 /2023, que têm como assunto:

Proposta de fiscalização com o objetivo de promover a melhoria na gestão de riscos de segurança da informação.

Com o seguinte sumário:

PROPOSTA DE FISCALIZAÇÃO. MODALIDADE OPERACIONAL. PROTEGE-TI 2023. VULNERABILIDADES DOS SERVIÇOS DE DOMÍNIO DO ACTIVE DIRECTORY. AUTORIZAÇÃO. ORIENTAÇÕES.

E com a seguinte descrição:

O objetivo da fiscalização é promover a melhoria na gestão de riscos de segurança da informação dos órgãos auditados no contexto dos Serviços de Domínio do Active Directory (AD-DS) da Microsoft, por meio da avaliação dos controles administrativos e técnicos existentes nas organizações a serem fiscalizadas.

6.12.1 - A COSEC entende que, devido a importância da segurança da informação e a necessidade de adoção de medidas preventivas para mitigar riscos cibernéticos, se faz necessário a aquisição de um módulo de gestão de vulnerabilidades para o Active Directory.

6.12.2 - O Active Directory (AD) é essencial para a nossa infraestrutura de TI, pois facilita a administração de recursos, políticas de segurança e controles de acesso. No entanto, sua complexidade e importância o tornam um alvo atrativo para atacantes. A gestão de vulnerabilidades é crucial para identificar, classificar, priorizar e corrigir proativamente as vulnerabilidades presentes no AD, garantindo a integridade e segurança dos nossos dados e sistemas.

6.12.3 - O acórdão do TCU nº 2265/2023 enfatiza que:

Devido a falhas de configurações dos Serviços de Domínio Active Directory (AD-DS) das organizações públicas poderá ocorrer o comprometimento dos domínios de rede das organizações, o que poderá levar à exfiltração, ao sequestro ou à destruição de informações por meio de ataques de ransomware e impactar negativamente a prestação de serviços públicos ao cidadão bem como a imagem da organização.

O que nos remete a necessidade de fortalecer a segurança cibernética nas organizações públicas, destacando que a falta de medidas adequadas pode resultar em graves consequências, como perda de dados sensíveis e interrupção de serviços essenciais.

6.12.4 - Dessa forma, a aquisição de um módulo de gestão de vulnerabilidades para Active Directory visa prover: identificação de fraquezas; ações preventivas de hardening; identificação de ataques específicos; análise detalhada de configurações incorretas; recomendações de correção, avaliação de relações de confiança perigosas entre florestas e domínios; captura de mudanças no AD; dashboard de ataques e vulnerabilidades; correlação de mudanças e desvios de segurança; análise de ataques com base no MITRE ATT&CK; gerenciamento por meio de interface web; criação de dashboards customizados; modelo de controle de acesso baseado em funções (RBAC) para garantir que apenas usuários autorizados tenham acesso às informações sensíveis; preservação da integridade do ambiente sem realizar alterações no AD; sem armazenamento de credenciais de modo a garantir a segurança das informações; suporte a múltiplas florestas e domínios; monitoramento contínuo; retenção de eventos; descoberta e mapeamento da superfície de ataque; validação contínua da postura de segurança; detecção e resposta a ataques; integração com SIEM; capacidade de criação de regras YARA; integração por meio de APIs REST; e listas de exclusões.

6.12.5 - A aquisição de um módulo de gestão de vulnerabilidades para Active Directory representa uma evolução funcional necessária em relação à solução anterior e uma medida estratégica alinhada às recomendações do TCU e às melhores práticas de segurança da informação. Essa iniciativa fortalecerá a postura de segurança da nossa organização, protegendo nossos sistemas contra ameaças cibernéticas e garantindo a integridade dos dados.

7. Estimativa da demanda - quantidade de bens e serviços

7.1- Área de negócio: Secretaria Geral

Grupo	Item	CATMAT / CATSER	Descrição	Unidade	Qtde.
	1	27502	Licença de uso de software /programa de proteção de endpoints do tipo Antimalware e EDR, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	2.150

1	2	27502	Licença de uso de software /programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	2.150
	3	27502	Licença de uso de software /programa de prevenção de perda de dados do tipo DLP, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	2.150
	4	27502	Solução de proteção de segurança de rede do tipo IPS (Tipo I), podendo ser somente a Licença de uso de software /programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.10 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças ou licenças e equipamentos	2
	5	27502	Licença de uso de software /programa de filtragem e proteção de e-mails do tipo Secure E-Mail Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	2.150
	6	27502	Licença de uso de software /programa de detecção e gerenciamento de vulnerabilidades, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	2.150

7	27502	Solução de proteção de segurança de rede do tipo Firewall (Tipo I), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.11 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças ou licenças e equipamentos	4
8	27502	Licença de uso de software /programa de detecção e impedimento de acesso privilegiado não autorizado a recursos críticos do tipo PAM, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	100

Tabela 1

7.1.1.1 - Para as soluções 1 (AntiMalware/EDR), 2 (Secure Web Gateway), 3 (DLP), 5 (Secure E-Mail Gateway) e 6 (Gerenciamento de Vulnerabilidade), foi considerada a quantidade de ativos na rede administrada pelo DETIC. As evidências da quantidade atual de ativos na rede administrada pelo DETIC, totalizando 2.104 estações, estão presentes na imagem 1.

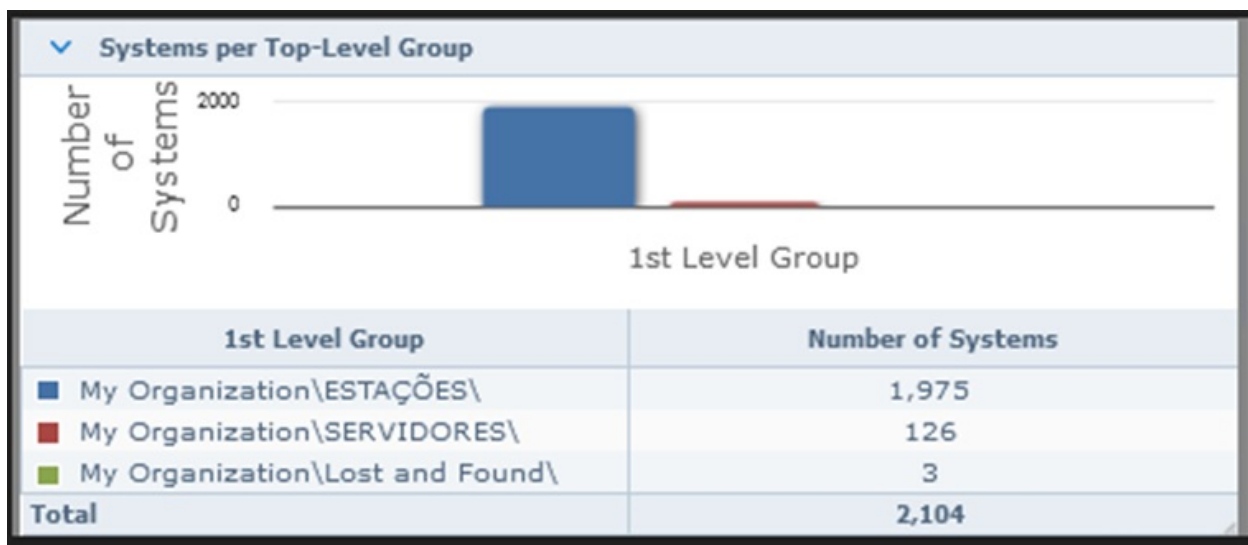


Imagem 1

Dessa forma, verificou-se a necessidade de aquisição de um total de 2.150 licenças para atender à demanda de segurança da rede ACMD. A diferença de 46 licenças deve-se a flutuações na demanda e margem para crescimento dos ativos.

7.1.2 - Para a solução 4 (IPS), foi considerada a quantidade de equipamentos IPS, atualmente suportados pelo Contrato vigente, nº 17/2022-MD (5663604). A rede administrativa da DETIC possui dois equipamentos IPS.

Realizada análise para avaliação da permanência dos dois equipamentos, modelo IPS-NS7500, atualmente disponíveis na rede ACMD, e foi verificado:

- a) Os equipamentos de IPS em questão continuam a operar de maneira eficiente, atendendo às necessidades de segurança da rede. A taxa de uso de troubleshooting entre 40% e 50% indica que o sistema está sendo monitorado e mantido adequadamente, sem apresentar falhas críticas que comprometam sua funcionalidade, conforme imagem abaixo.

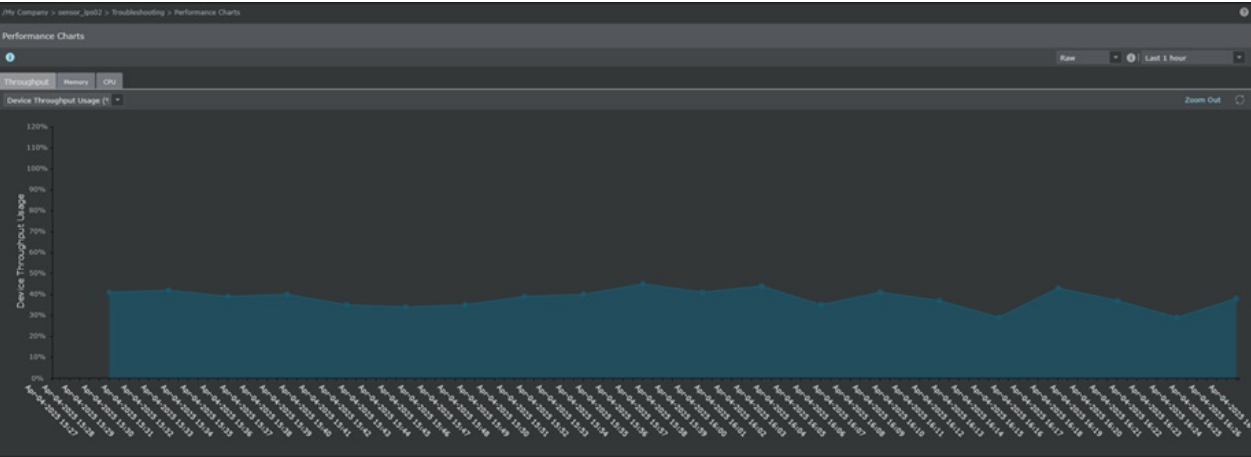


Imagem 2

- b) Considerando também que os equipamentos não irão atingir o End of Life (EOL) ou End of Support (EOS) do fabricante (<https://www.trellix.com/support/end-of-life-products/>) até 15/02/2030, manter os equipamentos é uma decisão financeiramente prudente, permitindo a otimização dos recursos disponíveis.

Hardware Products

Trellix Product	Model Number	End-of-Life Date
Intrusion Prevention System	NS 7500	2/15/2030
Intrusion Prevention System	NS 7150	12/31/2026
Intrusion Prevention System	NS 7250	12/31/2026
Intrusion Prevention System	NS 7350	12/31/2026
Intrusion Prevention System	NS 7500	2/15/2030

Imagem 3

Diante dos pontos apresentados, a manutenção dos equipamentos de IPS, juntamente com o quantitativo atual, atende plenamente às necessidades de segurança da rede ACMD. Portanto, a escolha de manter este quantitativo é justificada e adequada para garantir a proteção contínua e eficaz da infraestrutura de rede.

7.1.3 - Para a solução 7 (Firewall), foi considerada a quantidade de equipamentos Firewall, atualmente suportados pelo Contrato vigente, nº 17/2022-MD (5663604). A rede administrativa da DETIC possui quatro equipamentos Firewall Tipo I, visando a alta disponibilidade, com seguimento interno (duas unidades) e externo (duas unidades).

Realizada análise para avaliação da permanência dos quatro equipamentos Palo Alto, modelo/versão PA3410, atualmente disponíveis na rede ACMD, e foi verificado:

a) Os equipamentos de Firewall em questão continuam a operar de maneira eficiente, atendendo às necessidades de segurança da rede. A taxa de uso de troubleshooting abaixo de 20% indica que o sistema está sendo monitorado e mantido adequadamente, sem apresentar falhas críticas que comprometam sua funcionalidade, conforme imagens abaixo.

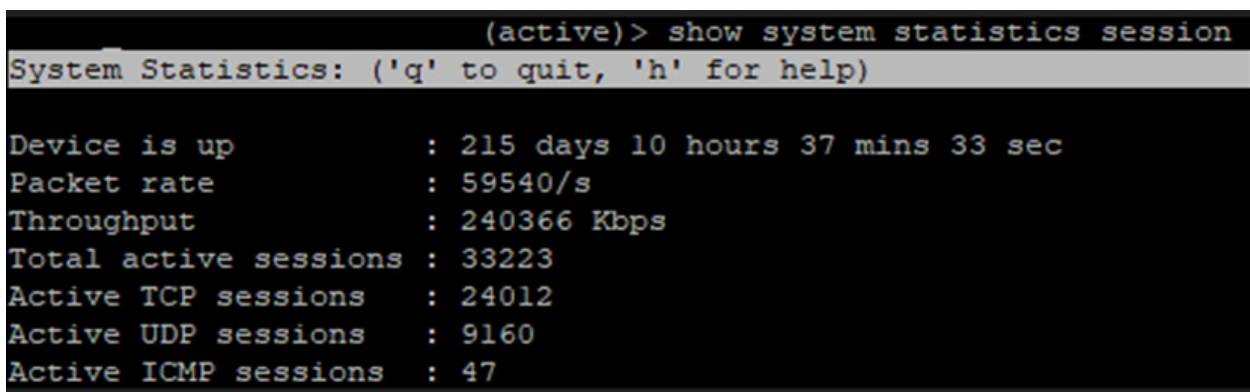


Imagem 4

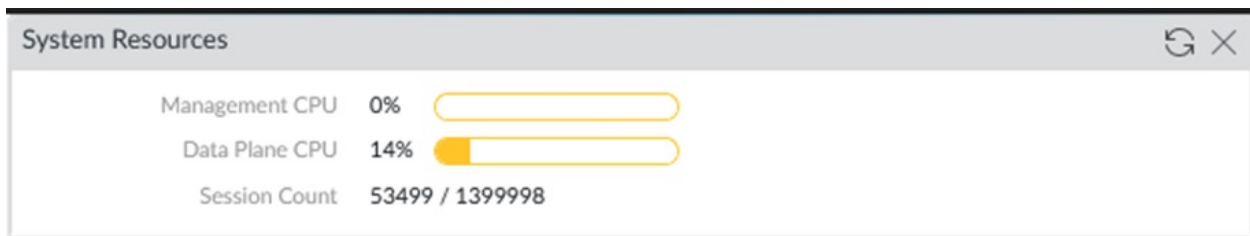


Imagem 5

b) Considerando também que os equipamentos ainda não têm previsão de atingir o End of Life (EOL) ou End of Support (EOS) do fabricante (<https://www.paloaltonetworks.com/services/support/end-of-life-announcements/hardware-end-of-life-dates>), manter os equipamentos é uma decisão financeiramente prudente, permitindo a otimização dos recursos disponíveis.

Diante dos pontos apresentados, a manutenção dos equipamentos de Firewall, juntamente com o quantitativo atual, atende plenamente às necessidades de segurança da rede ACMD. Portanto, a escolha de manter este quantitativo é justificada e adequada para garantir a proteção contínua e eficaz da infraestrutura de rede.

7.1.4 - Para a solução 8, foi considerado o quantitativo de usuários que possuem acesso privilegiado. Atualmente os usuários que possuem este privilégio são os que trabalham diretamente na DETIC. Desta forma, contabilizou o total de vagas dos servidores civis, militares e contratados que trabalham na DETIC, conforme tabela 2.

Num Ordem	Cargo	Abreviação	TIPO	Vínculo	Setor
1	Diretor	CCE-15	1.15	Servidor	Gabinete
2	Gerente/Coord Geral	CCE-13	1.13	Servidor	CGGOV
3	Gerente/Coord Geral	CCE-13	1.13	Servidor	CGSOL
4	Gerente/Coord Geral	CCE-13	1.13	Livre	CGINF
5	Coordenador	CCE-10	1.10	Servidor	COSEC
6	Coordenador	CCE-10	1.10	Servidor	CGGOV
7	Coordenador	CCE-10	1.10	Livre	CGSOL
8	Coordenador	CCE-10	1.10	Servidor	CGINF/COINS
9	Coordenador	CCE-10	1.10	Livre	CGINF/COTEL
10	Coordenador	CCE-10	1.10	Livre	CGINF/COGIN
11	Coordenador	CCE-10	1.10	Livre	CGINF/COSER
12	Coordenador	FCE-10	1.10	Servidor	CGINF/COSAU
13	Assistente	CCE-7	2.07	Livre	CGGOV

14	Assistente	CCE-7	2.07	Livre	CGGOV
15	Assistente	CCE-7	2.07	Servidor	CGSOL
16	Assistente	CCE-7	2.07	Livre	CGINF/COINS
17	Assistente	CCE-7	2.07	Livre	CGINF/COINS
18	Assistente	CCE-7	2.07	Livre	CGINF
19	Assistente	CCE-7	2.07	Livre	COSEC
20	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COSAU
21	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COTEL
22	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COINS
23	Assistente Técnico	CCE-5	2.05	Servidor	CGGOV
24	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COSAU
25	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COSAU
26	Assistente Técnico	CCE-5	2.05	Livre	CGINF/COSAU
27	Assistente Técnico	FCE-5	2.05	Servidor	CGINF/COTEL
28	Assistente Técnico Militar	GR	0005 (E)	FAB	COSEC
29	Assistente Técnico Militar	GR	0005 (E)	EB	CGINF/COGIN
30	Assistente Técnico Militar	GR	0005 (E)	MB	CGINF/COINS
31	Supervisor	Nível	V	EB	COSEC

32	Supervisor	Nível	V	EB	Gabinete
33	Supervisor	Nível	V	FAB	CGSOL
34	Supervisor	Nível	V	EB	CGINF/COTEL
35	Supervisor	Nível	V	MB	CGINF/COTEL
36	Supervisor	Nível	V	FAB	CGINF/COSAU
37	Supervisor	Nível	V	MB	Gabinete
38	Supervisor	Nível	V	MB	CGINF/COSAU
39	Supervisor	Nível	V	EB	CGINF/COSER
40	Especialista	Nível	II	MB	COSEC
41	Especialista	Nível	II	EB	CGGOV
42	Especialista	Nível	II	FAB	CGINF/COBDA
43	Especialista	Nível	II	EB	CGINF/COTEL
44	Assistente Técnico	FCE-3	2.03	Servidor	Gabinete
45	Assistente Técnico	FCE-3	2.03	Servidor	CGSOL
46	Assistente Técnico	FCE-3	2.03	Servidor	CGINF
47	Assistente Técnico Militar	GR	0005 (E)	MB	COSEC
48	Especialista	Nível	II	EB	CGSOL/super
49				EB	CGSOL/super

50				EB	CGGOV
51				EB	CGGOV
52				MB	CGGOV
53				FAB	CGINF/COSAU
54				FAB	CGINF/COGIN
55				EB	CGINF/COINS
56				EB	CGINF/COGIN
57				Terceirizado	Gabinete
58				Terceirizado	Gabinete/Copa
59				Terceirizado	Gabinete
60				Terceirizado	COSEC
61				Terceirizado	CGGOV
62				Terceirizado	CGSOL
63				Terceirizado	CGSOL/super
64				Terceirizado	CGINF
65				Terceirizado	CGINF/COSAU
66				Terceirizado	CGINF/COTEL
67				Terceirizado	CGINF/COINS
68				Terceirizado	Gabinete

69				Estagiário	CGGOV
70				Estagiário	CGSOL
71				Estagiário	CGSOL
72				Estagiário	CGSOL
73				Estagiário	CGSOL
74				Estagiário	CGSOL
75				Estagiário	CGSOL
76				Estagiário	CGSOL
77				Estagiário	CGINF/COGIN
78				Estagiário	CGINF/COGIN
79				Estagiário	CGINF/COSER
80				Estagiário	CGINF/COSER
81				Estagiário	CGINF/COINS
82				Estagiário	CGINF/COINS
83				Estagiário	CGINF/COSAU
84				Estagiário	CGINF/COSAU
85				Estagiário	CGINF/COSAU
86				Estagiário	CGINF/COSAU
87				Estagiário	CGINF/COSAU

88				Estagiário	CGINF/COSAU
89				Estagiário	CGINF/COSAU
90				Estagiário	CGINF/COSAU
91				Estagiário	CGINF/COSAU
92				Estagiário	CGINF/COSAU
93				Estagiário	CGINF/COSAU
94				Estagiário	CGINF/COSAU
95				Estagiário	CGINF/COSAU
96				Estagiário	CGINF/COSAU
97				Estagiário	CGINF/COTEL
98				Estagiário	CGINF/COTEL
99				Estagiário	CGINF/COTEL
100				Estagiário	CGINF/COTEL

Tabela 2

7.2- Área de negócio: EMCFA

Grupo	Item	CATMAT / CATSER	Descrição	Unidade	Qtde.
	1	27502	Licença de uso de software /programa de proteção de endpoints do tipo Antimalware e EDR, com instalação, configuração,	Licenças	250

1			suporte técnico e repasse de conhecimento.		
	2	27502	Licença de uso de software /programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	250
	3	27502	Licença de uso de software /programa de prevenção de perda de dados do tipo DLP, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças	250
	4	27502	Solução de prevenção e detecção de intrusão de rede do tipo IPS (Tipo II), sendo o conjunto completo de Licença de uso de software/programa com equipamentos, conforme subitem 6.10 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças e equipamentos	2
	5	27502	Solução de proteção de segurança de rede do tipo Firewall (Tipo II), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software /programa com equipamento, conforme subitem 6.11 , com instalação, configuração,	Licenças ou licenças e equipamentos	3

			suporte técnico e repasse de conhecimento.		
--	--	--	--	--	--

Tabela 3

7.2.1 - Para as soluções 1 (AntiMalware/EDR), 2 (Secure Web Gateway), 3 (DLP), foi considerado a quantidade média de usuários que acessam os serviços na rede administrada pela SC-1. Considerando que cada Operação Conjunta do EMCFA reúne aproximadamente 100 usuários, o quantitativo estimado torna-se capaz de suportar duas operações simultâneas com efetivo completo somado aos usuários permanentes da SC-1 (atualmente de 44 militares). Dessa forma, verificou-se a necessidade de aquisição de um total de 250 licenças para atender à demanda da ROD sem comprometer sua capacidade de receber usuários eventuais mantendo os níveis adequados de segurança. Vale ressaltar que a ROD é uma rede onde a grande maioria de usuários são eventuais e que, quando estes conectam-se à rede precisam adotar as medidas de segurança e/ou utilizar os dispositivos certificados para tal.

7.2.2 - Para a solução 4 (IPS), foi considerada a quantidade de equipamentos IPS necessários para prover uma efetiva proteção dos 2 canais de saída para a internet (TELEBRAS e SERPRO). Atualmente, a ROD não possui equipamentos IPS e tem-se observado a necessidade crescente de incrementarmos o nível de segurança dessas portas externas considerando os ataques cibernéticos sofridos por outras redes.

7.2.3 - Para a solução 5 (Firewall), foi considerada a quantidade de equipamentos Firewall atualmente mantidos via Contrato vigente, nº 17/2022-MD (5663604). A ROD possui 3 (três) equipamentos Firewall Tipo II (Fabricante: PaloAlto), visando a alta disponibilidade e que precisam ser mantidos para além do período coberto pelo contrato que expirará em setembro do corrente ano.

8. Levantamento de soluções

O levantamento das soluções buscou levar em consideração os seguintes itens:

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

a) Os demais Órgãos ou entidades da Administração pública federal igualmente possuem necessidades de manter dispositivos e sistemas que permitam garantir a segurança de seus ativos de tecnologia da informação, uma vez que tal atividade

reveste-se de importância para a manutenção de níveis aceitáveis de disponibilidade, integridade, confidencialidade e autenticidade de suas informações.

b) Dessa forma, foram observados nos levantamentos de preços realizados por meio de consulta ao Painel de Preços (<https://paineldeprescos.planejamento.gov.br/>), soluções semelhantes em outros órgãos e entidades da Administração Pública. Nesse levantamento, foram identificadas soluções de segurança da informação, baseadas em diversas tecnologias. No entanto, as topologias e arquiteturas adotados em cada órgão são configurados às suas necessidades, bem como às características de seus sistemas e ativos de TI, o que faz com que cada qual, incluindo-se as redes da ACMD e da ROD, possuam características e requisitos únicos e particulares.

8.2 - As alternativas do mercado:

a) As soluções levantadas baseiam-se em ferramentas de código livre, gratuitas, e solução de mercado composta por: licenças, contratação de instalação, configuração, suporte técnico e repasse de conhecimento ou a contratação das soluções na forma de serviço.

8.3 - A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28/09/2016, alterada pela Portaria SGD/ME nº 3, de 27/06/2019:

a) Foi realizada uma pesquisa no site (<https://softwarepublico.gov.br>), contudo não foi identificada nenhuma solução que atenda aos requisitos técnicos necessários.

8.4 - As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis:

a) Não se aplica.

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):

a) Não será necessária, tendo em vista a rede administrativa da ACMD, bem como a ROD já disporem de infraestrutura adequada para a implantação das soluções requeridas. Vale ressaltar que essas soluções já estão implementadas em ambas as estruturas de TI, e o que se pretende nessa contratação, é aquisição de novos

licenciamentos, bem como os respectivos suportes técnicos devido à impossibilidade de renovação dos atuais contratos. A exceção é apenas com os equipamentos de IPS da ROD.

8.6 - Os diferentes modelos de prestação do serviço:

a) A solução composta por equipamentos, licenças, suporte técnico e repasse de conhecimento poderá ser contratada na forma de aquisição dos bens ou fornecida na forma de serviço, com pagamentos mensais durante a vigência contratual. Para essas duas possibilidades, os equipamentos devem ser instalados e configurados nas dependências do MD, especificamente nos centros de processamento de dados do DETIC e da SC-1.

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

a) As soluções levantadas possuem especificações, composição e características de bens e serviços diferentes entre si, conforme as tabelas 1 e 3 do item 7.

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

a) Realizada avaliação neste ETP sobre a viabilidade de aquisição na forma de bens ou contratação como serviço. Esta análise está sendo conduzida especificamente no item 9 (Solução S-04 e Solução S-05). Na Solução S-04, está sendo considerada a possibilidade de adquirir as licenças e equipamentos das ferramentas de segurança, com a administração pelas equipes da COSEC e da SC-1, necessários para atender às demandas das redes ACMD e ROD. Já na Solução S-05, estamos avaliando a contratação dos serviços necessários para a execução das atividades por fornecedores que serão responsáveis pelas licenças e equipamentos de segurança e pela administração dos mesmos. A decisão final será baseada em critérios técnicos, econômicos, visando sempre a melhor solução para o Ministério da Defesa.

8.9 - A ampliação ou substituição da solução implantada:

a). As soluções levantadas visam a aquisição de novos licenciamentos, bem como a cobertura contratual de suporte técnico e repasse de conhecimento. O presente Estudo Técnico Preliminar visa analisar soluções para aquisição ou substituição das licenças já implementadas na rede administrativa da ACMD e na ROD, dessa forma as soluções a serem adquiridas e implementadas devem ter a sua capacidade e efetividade **iguais ou superiores às atuais**, ou seja, os requisitos técnicos serão baseados nas soluções que estão atualmente em funcionamento.

8.10- As diferentes métricas de prestação do serviço e de pagamento levantadas são:

- Contratação das licenças/equipamentos com prazo/validade estabelecidos de 12 meses e pagamento único;
- Contratação das licenças/equipamentos com prazo/validade estabelecidos de 36 meses e pagamento em três vezes (anual), de forma anual;
- Contratação das soluções na forma de serviço por 12 meses com pagamentos mensais durante a vigência contratual; e
- Contratação das soluções na forma de serviço por 36 meses com pagamentos mensais durante a vigência contratual.

Id	Descrição da solução (ou cenário)
S-01	Não efetuar a Contratação/Utilização de Ferramentas de Segurança.
S-02	Contratação/Utilização das Ferramentas de Segurança de Software Livre.
S-03	Utilização de Solução Própria desenvolvida internamente ao órgão.
S-04	Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança.
S-05	Contratação das Soluções na Forma de Serviço para Contratação /Utilização de Ferramentas de Segurança.

Tabela 4

9. Análise comparativa de soluções

Requisitos		Cenários				
		S-01	S-02	S-03	S-04	S-05
	A solução encontra-se implantada em					

Negócio	outro órgão ou entidade da Administração Pública?	Não atende	Atende	Não atende	Atende	Atende
	A solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Não atende	Não atende	Não atende	Não atende	Não atende
	A solução é composta por software livre ou software público? (quando se tratar de software)	Não atende	Atende	Não atende	Não atende	Não atende
	A solução mantém a estrutura atual, reduzindo os custos com treinamento da equipe técnica e tempo para adaptação a nova Ferramenta	Não atende	Não atende	Não atende	Atende	Atende
	A solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Não atende	Não atende	Não atende	Atende	Atende

Tecnológico	A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Não se aplica	Não se aplica	Não se aplica	Não se aplica	Não se aplica
	A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Não se aplica	Não se aplica	Não se aplica	Não se aplica	Não se aplica
Resultado da Análise		não viável	não viável	não viável	viável	viável

Tabela 5

Solução S-01 – Não efetuar a Contratação/Utilização de Ferramentas de Segurança.

Descrição: Esta solução propõe não realizar um novo procedimento licitatório para a contratação de ferramentas de segurança destinadas à proteção das redes ACMD e ROD.

Análise: O contrato de licenciamento e suporte técnico das ferramentas de segurança atualmente vigente no Ministério da Defesa expira em **29/09/2025**. Caso não seja realizada uma nova contratação por meio de um processo licitatório, as ferramentas deixarão de receber atualizações, que incluem melhorias e novas funcionalidades, além de perderem o suporte técnico do fabricante para defeitos e vulnerabilidades.

Embora essa solução possa parecer economicamente vantajosa à primeira vista, ela é inviável, pois manter as redes ACMD e ROD desprotegidas resultará em custos elevados para a recuperação do ambiente computacional após um possível ataque cibernético, além dos danos à imagem institucional. Esses ataques podem ser desencadeados por ameaças virtuais em ativos computacionais sem uma solução de segurança instalada ou sem manutenção e atualizações contínuas fornecidas pelo fabricante.

Solução S-02 – Contratação/Utilização das Ferramentas de Segurança de Software Livre.

Descrição: Software Livre é conceituado como qualquer programa de computador que pode ser usado, copiado, estudado, modificado e redistribuído sem nenhum tipo de restrição. Assim, além da sua utilização não estar vinculada ao pagamento de direitos autorais, a principal característica do Software Livre está na distribuição com o código fonte aberto, dando permissão a qualquer usuário de modificá-lo e adaptá-lo às suas necessidades individuais.

Análise: Ao considerar a utilização de diversas ferramentas *open-source* para atender às necessidades do negócio, percebe-se que, embora o custo envolvido seja mínimo devido ao uso de ferramentas gratuitas, o tempo necessário para pesquisa, desenvolvimento, implementação e integração de todas as ferramentas inviabiliza essa opção.

Além disso, é importante destacar que o DETIC e o SC-1 não possuem profissionais com as qualificações necessárias para implementar e integrar os softwares requeridos para atender às demandas listadas no item 7 deste estudo. Outro ponto crucial é que nem todas as funcionalidades necessárias são oferecidas por ferramentas *open-source*, muitas das quais possuem versões gratuitas com funcionalidades bastante limitadas. Nesse cenário, a atualização das ferramentas também não é garantida pela comunidade e pode recair como obrigação para uma possível equipe de desenvolvimento interno ao MD.

Por fim, há também a preocupação com a possibilidade de códigos maliciosos serem inseridos intencionalmente nessas ferramentas por colaboradores, criando brechas para invasões e execução de código remoto.

Solução S-03 – Utilização de Solução Própria Desenvolvida Internamente ao Órgão.

Descrição: Solução das ferramentas de segurança desenvolvidas pela própria organização, sem a necessidade de uma contratação.

Análise: Esta solução é inviável devido à falta de pessoal especializado e às dificuldades de desenvolver sistemas dessa complexidade com recursos humanos e materiais próprios. Mesmo que fosse possível, a integração com as soluções atualmente utilizadas no MD seria inviável devido à complexidade desses sistemas. O tempo necessário para desenvolvimento de tais soluções, que normalmente é muito extenso por conta da complexidade tecnológica, também inviabiliza esta linha de ação tendo em vista que as ferramentas atuais vencem em setembro do corrente ano.

Além disso, é importante destacar que sistemas e ferramentas de segurança de TI exigem constante atualização de modo a fazer face às novas ameaças e demandaria uma constante manutenção das ferramentas e uma equipe de desenvolvimento capacitada e permanente para tal serviço.

Solução S-04 – Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança.

Descrição: A contratação ou utilização de aplicativos de mercado para ferramentas de segurança envolve a aquisição de licença de software de segurança desenvolvido por empresas especializadas. Essas ferramentas são projetadas para proteger sistemas e dados contra ameaças cibernéticas, oferecendo diversas funcionalidades de segurança.

Análise: A utilização de licenças de mercado para ferramentas de segurança é uma prática comum entre organizações que buscam garantir a proteção de seus ativos digitais. Essas ferramentas são desenvolvidas por fornecedores que investem continuamente em pesquisa e desenvolvimento para aprimorar suas soluções e responder às novas ameaças cibernéticas. A análise dessa solução está considerando os aspectos de custo (item 11), eficácia, facilidade de implementação e suporte técnico.

Os principais pontos a serem protegidos são os endpoints com a utilização de sistema de Antimalware, EDR e DLP, as redes ACMD e ROD, com a utilização de sistemas de Secure Web Gateway, Secure E-Mail Gateway, verificação de vulnerabilidade, IPS, Firewall e PAM.

Adicionalmente foi realizada também uma avaliação dos equipamentos físicos dos produtos já existentes, que incluem 02 (dois) equipamentos IPS da rede ACMD, 04 (quatro) equipamentos de Firewall da rede ACMD e 03 (três) equipamentos de Firewall da rede ROD. Tais equipamentos, após análise de carga e desempenho, conforme subitens 7.1.2 e 7.1.3, mostraram-se ainda suficientes para a atual estrutura das redes

envolvidas. Desse modo, a manutenção deles ainda é viável como objetivo de redução de custos.

Outra avaliação considerou o custo de aquisição de novos equipamentos em comparação com a renovação das licenças de uso de software/programa. Conforme a tabela abaixo, o custo para a troca dos 02 equipamentos de IPS em uma avaliação de 12 meses corresponde a um acréscimo de 41,54% em relação apenas a renovação de licença. Esta diferença reduz quando colocado para um período temporal de 36 meses, uma vez que o hardware permanece o mesmo. Porém a solução com um novo equipamento ainda terá um acréscimo de 20,77% em relação apenas a licença de uso. Os valores para os Firewall da rede ACMD e da ROD seguem com porcentagens próximas ao apresentado no estudo do IPS (Firewall ACMD para 12 meses 44,44% e 36 meses 21,05% e Firewall ROD para 12 meses 42,86% e 36 meses 20,00%).

Portanto, será mais vantajoso para o MD optar pela renovação das licenças de uso. No entanto, visando ampliar a competitividade, será permitido que os participantes da licitação forneçam novos equipamentos de outros fabricantes, atendendo aos requisitos definidos no Anexo I deste ETP, com a inclusão das licenças de uso.

Solução	Valor do Equipamento e da Licença de uso	Valor apenas da Licença de uso	Diferença em percentual
02 unidades do IPS-NS7500 para 12 meses	R\$ 1.300.000,00	R\$ 760.000,00	41,54%
02 unidades do IPS-NS7500 para 36 meses	R\$ 2.600.000,00	R\$ 2.060.000,00	20,77%
04 unidades de Firewall PA-3410 para 12 meses	R\$ 1.080.000,00	R\$ 600.000,00	44,44%
04 unidades de Firewall PA-3410 para 36 meses	R\$ 2.280.000,00	R\$ 1.800.000,00	21,05%
03 unidades de Firewall PA-850 para 12 meses	R\$ 630.000,00	R\$ 360.000,00	42,86%

03 unidades de Firewall PA-850 para 36 meses	R\$ 1.350.000,00	R\$ 1.080.000,00	20,00%
--	------------------	------------------	--------

Tabela 6

Os valores constantes da tabela 06 estão disponíveis como documento do SEI número 7914185 deste ETP.

Por fim, esta solução apresenta-se como viável para o órgão e possui algumas vantagens e desvantagens, listadas a seguir.

Vantagens:

Atualizações Regulares pelo Fabricante: Ferramentas licenciadas recebem atualizações frequentes, garantindo proteção contra as ameaças mais recentes.

Suporte Técnico Especializado: Empresa contratada para fornecer a solução irá fornecer suporte técnico especializado, auxiliando na resolução de problemas e na otimização do uso das ferramentas.

Conformidade com Regulamentações: Ferramentas licenciadas ajudam a garantir a conformidade com regulamentações de segurança e proteção de dados, como a LGPD.

Funcionalidades Avançadas: Soluções de mercado geralmente oferecem funcionalidades avançadas que não estão disponíveis em ferramentas *open-source* (software livre).

Redução de Riscos: A utilização de ferramentas de segurança licenciadas reduz os riscos de vulnerabilidades e ataques cibernéticos.

Manutenção da Compatibilidade com o atual Sistema de Segurança das redes ACMD e ROD: A utilização das ferramentas de segurança já em uso permite a manutenção do conhecimento técnico da equipe, reduzindo os custos de treinamento, implantação e diminuindo o tempo necessário para solucionar um ataque cibernético.

Equipamentos e Licenças de Propriedade do Órgão: não há o risco de descontinuidade dos serviços caso haja interrupção do contrato ou a falência da empresa contratada.

Desvantagens:

Custo: A aquisição de licenças de mercado representa um custo alto em virtude das funcionalidades avançadas, da manutenção preventiva e corretiva, do suporte técnico e do valor cotado, normalmente, em dólares americanos.

Pagamento no Início do Contrato: Normalmente, o desembolso do valor total do contrato deverá ser feito no ato da contratação.

Solução S-05 – Contratação das Soluções na Forma de Serviço para Contratação /Utilização de Ferramentas de Segurança.

Descrição: A contratação de soluções de segurança na forma de serviço, também conhecida como Security as a Service (SECaaS), envolve a terceirização de serviços de segurança para um provedor especializado. Esses serviços são alocados diretamente no órgão para utilização local, ou em nuvem, durante o período de vigência contratual.

Análise: A empresa selecionada será responsável pela aquisição das licenças e dos equipamentos de segurança, disponibilizando-os diretamente no órgão ou por meio de um provedor na nuvem. Essa empresa cuidará da configuração, implementação e manutenção das soluções de segurança, adaptando-as às necessidades específicas do órgão. Os serviços poderão ser acessados e gerenciados tanto por interfaces locais quanto na nuvem, permitindo monitoramento e suporte contínuos. Essa abordagem se mostra viável para o órgão, apresentando algumas vantagens e desvantagens, conforme listado a seguir:

Vantagens:

Baixo Custo no Início do Contrato: Reduz a necessidade de investimentos iniciais altos, uma vez que os desembolsos são mensais, durante o período contratual.

Acesso a Tecnologias Avançadas: Permite o acesso a tecnologias de ponta sem a necessidade de atualizações constantes.

Suporte Especializado: Profissionais especializados oferecem suporte técnico contínuo e monitoramento ativo.

Desvantagens:

Solução de Alto Risco: Os equipamentos e as licenças são de propriedade da empresa o que requer uma estratégia de mitigação de perdas de dados e continuidade dos serviços caso haja interrupção do contrato ou da prestação de serviço.

Custo Elevado: Contratos com empresas de Security as a Service (SECaaS) geralmente são bastante onerosos devido aos custos associados ao pagamento de

licenças (geralmente em dólares americanos), aquisição de equipamentos, manutenção de uma equipe técnica especializada, tecnologias proprietárias e únicas, e a necessidade de disponibilidade proativa desses profissionais.

Confiança e Controle de Dados: Contratar uma empresa terceirizada para gerenciar a segurança cibernética do órgão pode gerar preocupações significativas em relação à confiança. Ao terceirizar, você está essencialmente entregando o controle total dos seus dados sensíveis a terceiros. Isso pode aumentar o risco de vazamento de informações, uso indevido de dados e falta de transparência sobre como os dados estão sendo protegidos. Manter a segurança da informação internamente permite um controle mais rigoroso e direto sobre quem tem acesso aos dados e como eles são gerenciados, reduzindo assim os riscos associados à confiança em terceiros. Além disso, muitas ferramentas oferecidas no mercado funcionam exclusivamente na nuvem e pode levar a uma maior exposição dos dados organizacionais.

Dependência de Terceiros: O órgão fica dependente do provedor para a gestão e manutenção das soluções de segurança, podendo gerar riscos em garantir que a empresa cumpra todas as regulamentações e normas de segurança determinadas.

Pessoal Especializado para Fiscalização: Pelas características das ferramentas disponibilizadas nesse modelo de contratação, o órgão contratante necessitará de profissionais especializados na gestão e fiscalização contratual, responsáveis por realizar análises técnicas, validar as atividades da empresa e gerenciar os pagamentos mensais.

10. Registro de soluções consideradas inviáveis

As soluções S-01, S-02 e S-03 são consideradas inviáveis, tendo em vista os motivos expostos em suas respectivas análises no item 9.

11. Análise comparativa de custos (TCO)

Para as soluções técnica e funcionalmente viáveis, que são as soluções S-04 e S-05, foram realizados os comparativos dos custos totais de propriedade, a seguir:

11.1 - CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Foram realizadas pesquisas de preços visando a estimativa de custos para a solução S-04 (Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança) e para a solução S-05 (Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança).

Para a solução S-04, foram encontrados alguns contratos similares com a APF que contemplam as soluções objeto deste ETP, contudo, por conterem quantitativos e prazos distintos, foram considerados os valores unitários e os prazos de 12 meses e 36

meses. De forma adicional, foram realizadas consultas à empresas do ramo, solicitando estimativa de custos para as soluções demandadas. Todos os valores levantados para a solução S-04 foram consolidados nas tabelas 7 e 8, conforme abaixo:

Solução Viável 1 (Solução S-04) – Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança para 12 meses – VALOR UNITÁRIO						
Orçamentos /Consulta Comprasnet -->	1 ORÇAMENTO 1 (Global) (7914173)	2 ORÇAMENTO 2 (Fasthelp) (7914181)	3 ORÇAMENTO 3 (Layer) (7914184)	4 PE 90216 /2024 UASG 943001 (7908350)	5 PE 90013 /2024 UASG 926646 (7910032)	6 PE 90040 /2024 UASG 925866 (7910049)
1 - Proteção de endpoints do tipo Antimalware/EDR	R\$ 180,00	R\$ 261,84	R\$ 433,00	R\$ 580,00		
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	R\$ 120,00	R\$ 299,23	R\$ 141,00			
3 - Prevenção de perda de dados do tipo DLP	R\$ 80,00	R\$ 95,63	R\$ 102,00		R\$ 480,00	
4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	R\$ 385.000,00	R\$ 305.326,77	R\$ 440.000,00			
5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II		R\$ 236.428,44	R\$ 950.000,00			
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	R\$ 110,00	R\$ 138,13	R\$ 285,00			
7 – Detecção e gerenciamento de vulnerabilidades	R\$ 320,00	R\$ 190,32	R\$ 400,00			

8 - Proteção de segurança de rede do tipo Firewall – Tipo I	R\$ 150.000,00	R\$ 175.527,36	R\$ 160.000,00			
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	R\$ 10.000,00	R\$ 17.202,90	R\$ 11.300,00			R\$ 14.895,85
10 - Proteção de segurança de rede do tipo Firewall – Tipo II		R\$ 83.054,49	R\$ 77.500,00			

Tabela 7

Solução Viável 1 (Solução S-04) – Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança para 36 meses – VALOR UNITÁRIO										
Orçamentos /Consulta Comprasnet -->	1	2	3	4	5	6	7	8	9	10
	ORÇAMENTO 1 (Global) (7914173)	ORÇAMENTO 2 (Fasthelp) (7914181)	ORÇAMENTO 3 (Layer) (7914184)	PE 90006/2024 UASG 990141 (7910027)	PE 0032 /2023 UASG 070006 (7910028)	PE 90006 /2024 UASG 990141 (7910033)	PE 90007 /2024 UASG 153019 (7910036)	PE 00060 /2023 UASG 070001 (7910041)	PE 90026 /2024 UASG 183023 (7910045)	PE 90009 /2024 UASG 925480 (7910052)
1 - Proteção de endpoints do tipo Antimalware/EDR	450,00	464,86	1.494,00	489,60						
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	300,00	690,63	487,00		745,00					
3 - Prevenção de perda de dados do tipo DLP	200,00	237,07	352,00			200,00				
			1.518.000,00							

4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	1.039.500,00	760.295,40								
5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II		312.316,32	1.750.000,00							
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	800,00	345,32	984,00				169,69			
7 – Detecção e gerenciamento d e vulnerabilidades	800,00	475,87	1.180,00					995,00		
8 - Proteção de segurança de rede do tipo Firewall – Tipo I	375.000,00	438.818,41	462.000,00						628.000,00	
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	25.000,00	39.699,25	29.600,00							21.900,00
10 - Proteção de segurança de rede do tipo Firewall – Tipo II		191.664,30	267.375,00							

Tabela 8

Todos os levantamentos foram realizados por meio de consultas ao sistema banco de preços (<https://www.bancodeprecos.com.br>), ao sistema painel de preços (<https://paineldeprecos.planejamento.gov.br>) e complementados por meio de cotações junto à empresas especializadas. Os valores estão disponíveis no SEI com o número correspondente do documento abaixo dos títulos de cada coluna.

Na estimativa de custo realizada para a solução S-04, utilizou como parâmetro o menor dos valores obtidos de cada item. Segue abaixo o resultado final para 12 meses e para 36 meses:

Solução Viável 1 (Solução S-04) – Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança – VALOR TOTAL pelas Opções 12 e 36 meses							
Pagamento para 12 meses				Pagamento para 36 meses			
Solução	Qtd	Valor Unitário	Valor Total	Solução	Qtd	Valor Unitário	Valor Total
1 - Proteção de endpoints do tipo Antimalware/EDR	2.400	R\$ 180,00	R\$ 432.000,00	1 - Proteção de endpoints do tipo Antimalware/EDR	2.400	R\$ 450,00	R\$ 1.080.000,00
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	2.400	R\$ 120,00	R\$ 288.000,00	2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	2.400	R\$ 300,00	R\$ 720.000,00
3 - Prevenção de perda de dados do tipo DLP	2.400	R\$ 80,00	R\$ 192.000,00	3 - Prevenção de perda de dados do tipo DLP	2.400	R\$ 200,00	R\$ 480.000,00
4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	2	R\$ 305.326,77	R\$ 610.653,54	4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	2	R\$ 760.295,40	R\$ 1.520.590,80
5 - Prevenção e detecção de intrusão de rede	2	R\$ 236.428,44	R\$ 472.856,88	5 - Prevenção e detecção de intrusão de rede	2	R\$ 312.316,32	R\$ 624.632,64

do tipo IPS – Tipo II				do tipo IPS – Tipo II			
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	2.150	R\$ 110,00	R\$ 236.500,00	6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	2.150	R\$ 169,69	R\$ 364.833,50
7 – Detecção e gerenciamento de vulnerabilidades	2.150	R\$ 190,32	R\$ 409.188,00	7 – Detecção e gerenciamento de vulnerabilidades	2.150	R\$ 475,87	R\$ 1.023.120,50
8 - Proteção de segurança de rede do tipo Firewall – Tipo I	4	R\$ 150.000,00	R\$ 600.000,00	8 - Proteção de segurança de rede do tipo Firewall – Tipo I	4	R\$ 375.000,00	R\$ 1.500.000,00
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	100	R\$ 10.000,00	R\$ 1.000.000,00	9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	100	R\$ 21.900,00	R\$ 2.190.000,00
10 - Proteção de segurança de rede do tipo Firewall – Tipo II	3	R\$ 77.500,00	R\$ 232.500,00	10 - Proteção de segurança de rede do tipo Firewall – Tipo II	3	R\$ 191.664,30	R\$ 574.992,90
Total (12 meses)			R\$ 4.473.698,42	Total (36 meses)			R\$ 10.078.170,34

Tabela 9

Com relação à solução S-05, não foi possível obter nos sistemas consultados, contratos semelhantes que contemplassem todas as soluções ofertadas na forma de serviços. Portanto, para a estimativa de custos dessa solução, foram realizadas consultas por e-mail com algumas empresas do ramo, onde foi solicitada uma estimativa de preços baseada nas necessidades do MD. Todos os valores levantados para a solução S-05 foram consolidados nas tabelas 10 e 11, para 12 e 36 meses, conforme abaixo:

Solução Viável 2 (Solução S-05) – Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança para 12 meses, pagamento mensal			
Orçamentos -->	1 ORÇAMENTO 1 (Global) (7914173)	2 ORÇAMENTO 2 (Fasthelp) (7914181)	3 ORÇAMENTO 3 (Layer) (7914184)
1 - Proteção de endpoints do tipo Antimalware/EDR	R\$ 580.500,00	R\$ 675.702,00	R\$ 1.872.000,00
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	R\$ 387.000,00	R\$ 771.936,00	R\$ 609.600,00
3 - Prevenção de perda de dados do tipo DLP	R\$ 258.000,00	R\$ 246.725,40	R\$ 441.600,00
4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	R\$ 1.155.000,00	R\$ 1.465.568,40	R\$ 1.584.000,00
5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II		R\$ 614.713,94	R\$ 3.420.000,00
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	R\$ 354.750,00	R\$ 356.556,00	R\$ 1.102.950,00
7 – Detecção e gerenciamento de vulnerabilidades	R\$ 1.032.000,00	R\$ 491.232,00	R\$ 1.548.000,00
8 - Proteção de segurança de rede do tipo Firewall – Tipo I	R\$ 900.000,00	R\$ 842.531,32	R\$ 1.152.000,00
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	R\$ 1.500.000,00	R\$ 2.064.348,00	R\$ 2.034.000,00
10 - Proteção de segurança de rede do tipo Firewall – Tipo II		R\$ 298.996,16	R\$ 418.500,00

Tabela 10

Solução Viável 2 (Solução S-05) – Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança para 36 meses, pagamento mensal			
Orçamentos -->	1 ORÇAMENTO 1 (Global) (7914173)	2 ORÇAMENTO 2 (Fasthelp) (7914181)	3 ORÇAMENTO 3 (Layer) (7914184)
1 - Proteção de endpoints do tipo Antimalware/EDR	R\$ 1.567.350,00	R\$ 1.199.700,00	R\$ 4.840.800,00
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	R\$ 1.044.900,00	R\$ 1.781.825,40	R\$ 1.579.200,00
3 - Prevenção de perda de dados do tipo DLP	R\$ 696.600,00	R\$ 611.640,60	R\$ 1.142.400,00
4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	R\$ 3.118.500,00	R\$ 3.649.417,92	R\$ 4.098.600,00
5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II		R\$ 812.022,48	R\$ 4.725.000,00
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	R\$ 957.825,00	R\$ 890.925,60	R\$ 2.857.350,00
7 – Detecção e gerenciamento de vulnerabilidades	R\$ 2.786.400,00	R\$ 1.227.744,60	R\$ 3.424.950,00
8 - Proteção de segurança de rede do tipo Firewall – Tipo I	R\$ 2.430.000,00	R\$ 2.106.328,36	R\$ 2.494.800,00
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	R\$ 4.050.000,00	R\$ 4.763.910,00	R\$ 3.996.000,00

10 - Proteção de segurança de rede do tipo Firewall – Tipo II	R\$ 689.991,48	R\$ 1.082.871,00
---	----------------	------------------

Tabela 11

Os valores estão disponíveis no SEI com o número correspondente do documento abaixo dos títulos de cada coluna.

Adicionalmente, para a Solução Viável 1 (Solução S-04) – “Contratação/Utilização de Licenças de Mercado para Ferramentas de Segurança”, foi realizado um levantamento junto a empresas fornecedoras dos produtos, conforme demonstrado na tabela abaixo, com o objetivo de verificar a existência de eventual economia significativa na adoção da modalidade de pagamento anual em comparação à modalidade de pagamento mensal. Essa análise foi conduzida em conformidade com o subitem 22.1.1 da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Empresa	Valor Total para 12 Meses pagamento ANUAL (A)	Valor Total para 12 Meses pagamento MENSAL (B)	Percentual de diferença entre ANUAL e MENSAL (C)
Fast Security	R\$ 6.845.016,18	R\$ 8.297.892,11	21,23%
VANELOS TECNOLOGIA	R\$ 5.421.677,00	R\$ 7.877.760,00	45,30%
GLOBAL SEC	R\$ 4.876.900,00	R\$ 7.236.000,00	48,37%
VTECH Segurança da Informação	R\$ 5.370.650,00	R\$ 7.992.000,00	48,81%
Shield Security	R\$ 5.616.951,48	R\$ 8.436.156,00	50,19%

Os valores estão disponíveis no SEI (8055757).

Fórmula – $C = (B-A)/A$

Constatou-se uma economia significativa com a adoção da modalidade de pagamento anual, superando o percentual de 12% previsto no subitem 22.1.1 da Portaria SGD /MGI nº 5.950/2023. Além da vantagem econômica, essa modalidade também contribui para a redução da carga de trabalho interno no Ministério da Defesa, ao eliminar a necessidade de processamento mensal dos pagamentos.

Na estimativa de custo realizada para a Solução S-05, utilizou-se como parâmetro o menor dos valores unitários mensais obtidos de cada item. Segue abaixo o resultado final da estimativa realizada tanto para 12 meses, quanto para 36 meses:

Solução Viável 2 (Solução S-05) – Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança – VALOR TOTAL pelas Opções 12 e 36 meses			
Pagamento para 12 meses		Pagamento para 36 meses	
Solução	Valor Total	Solução	Valor Total
1 - Proteção de endpoints do tipo Antimalware/EDR	R\$ 580.500,00	1 - Proteção de endpoints do tipo Antimalware/EDR	R\$ 1.199.700,00
2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	R\$ 387.000,00	2 - Filtragem e proteção de navegação Web do tipo Secure Web Gateway	R\$ 1.044.900,00
3 - Prevenção de perda de dados do tipo DLP	R\$ 246.725,40	3 - Prevenção de perda de dados do tipo DLP	R\$ 611.640,60
4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	R\$ 1.155.000,00	4 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo I	R\$ 3.118.500,00
5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II	R\$ 614.713,94	5 - Prevenção e detecção de intrusão de rede do tipo IPS – Tipo II	R\$ 812.022,48
6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	R\$ 354.750,00	6 - Filtragem e proteção de e-mails do tipo Secure E-Mail Gateway	R\$ 890.925,60
7 – Detecção e gerenciamento de vulnerabilidades	R\$ 491.232,00	7 – Detecção e gerenciamento de vulnerabilidades	R\$ 1.227.744,60
	R\$ 842.531,32		

8 - Proteção de segurança de rede do tipo Firewall – Tipo I		8 - Proteção de segurança de rede do tipo Firewall – Tipo I	R\$ 2.106.328,36
9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	R\$ 1.500.000,00	9 - Detecção e impedimento de acesso privilegiado não autorizado do tipo PAM	R\$ 3.996.000,00
10 - Proteção de segurança de rede do tipo Firewall – Tipo II	R\$ 298.996,16	10 - Proteção de segurança de rede do tipo Firewall – Tipo II	R\$ 689.991,48
Total (12 meses)	R\$ 6.471.448,82	Total (36 meses)	R\$ 15.697.753,12

Tabela 12

11.2 - MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Solução S-04 (12 meses)	R\$ 4.473.698,42	R\$ 4.473.698,42	R\$ 4.473.698,42	R\$ 13.421.095,26
Solução S-04 (36 meses)	R\$ 3.359.390,11	R\$ 3.359.390,11	R\$ 3.359.390,11	R\$ 10.078.170,34
Solução S-05 (12 meses)	R\$ 6.471.448,82	R\$ 6.471.448,82	R\$ 6.471.448,82	R\$ 19.414.346,46
Solução S-05 (36 meses)	R\$ 5.232.584,37	R\$ 5.232.584,37	R\$ 5.232.584,37	R\$ 15.697.753,12

Tabela 13

Para a Solução S-04, com validade de 12 meses, o custo total de propriedade após 36 meses (3 anos) de contrato é de R\$ 13.421.095,26.

Para a Solução S-04, com validade de 36 meses, o custo total de propriedade após 36 meses (3 anos) é de R\$ 10.078.170,34.

Para a Solução S-05, com validade de 12 meses, o custo total de propriedade após 36 meses (3 anos) de contrato é de R\$ 19.414.346,46.

Para a Solução S-05, o custo total de propriedade após 36 meses (3 anos) de contrato é de R\$ 15.697.753,12.

12. Descrição da solução de TIC a ser contratada

12.1 – Seleção da melhor Solução:

Após as análises das soluções realizadas nos itens 9 (Análise Comparativa das Soluções) e 11 (Análise Comparativa de Custos (TCO)), verificou-se que a Solução S-04 - Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança é a que melhor atende aos requisitos apresentados neste estudo. Esta solução oferece diversos benefícios e vantagens em comparação à Solução S-05 - Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança, conforme será demonstrado na Justificativa Técnica da Escolha da Solução (item 14) e na Justificativa Econômica da Escolha da Solução (item 15).

Solução de segurança cibernética para proteção da rede da ACMD e da ROD, composta pelos seguintes itens:

Grupo	Item	CATMAT / CATSER	Descrição	Unidade	Qtde.
	1	27502	Licença de uso de software /programa de proteção de endpoints do tipo Antimalware e EDR, com	Licenças /subscrição por 36 meses	2.400

1			instalação, configuração, suporte técnico e repasse de conhecimento.		
	2	27502	Licença de uso de software /programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças /subscrição por 36 meses	2.400
	3	27502	Licença de uso de software /programa de prevenção de perda de dados do tipo DLP, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças /subscrição por 36 meses	2.400
	4	27502	Solução de prevenção e detecção de intrusão de rede do tipo IPS (Tipo I), podendo ser somente a Licença de uso de software /programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.10 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças ou licenças e equipamentos /subscrição por 36 meses	2
	5	27502	Solução de prevenção e detecção de intrusão de rede do tipo IPS (Tipo II), sendo o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.10 , com instalação,	Licenças e equipamentos /subscrição por 36 meses	2

			configuração, suporte técnico e repasse de conhecimento.		
2	6	27502	Licença de uso de software /programa de filtragem e proteção de e-mails do tipo Secure E-Mail Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças /subscrição por 36 meses	2.150
3	7	27502	Licença de uso de software /programa de detecção e gerenciamento de vulnerabilidades, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças /subscrição por 36 meses	2.150
4	8	27502	Solução de proteção de segurança de rede do tipo Firewall (Tipo I), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software /programa com equipamento, conforme subitem 6.11 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças ou licenças e equipamentos /subscrição por 36 meses	4
5	9	27502	Licença de uso de software /programa de detecção e impedimento de acesso privilegiado não autorizado a recursos críticos do tipo PAM, com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças /subscrição por 36 meses	100

6	10	27502	Solução de proteção de segurança de rede do tipo Firewall (Tipo II), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software /programa com equipamento, conforme subitem 6.11 , com instalação, configuração, suporte técnico e repasse de conhecimento.	Licenças ou licenças e equipamentos /subscrição por 36 meses	3
---	----	-------	--	--	---

Tabela 14

12.2 – Agrupamento da solução:

Em que pese as soluções de segurança de TI demandadas serem autônomas, ou seja, uma solução não afeta tecnicamente a outra, as soluções que contém os itens 01, 02, 03, 04 e 05 devem funcionar de forma integrada, conforme as justificativas técnicas fornecidas no subitem 6.3 deste ETP. Pelo exposto elas devem ser agrupadas e adquiridas do mesmo fornecedor, compondo um grupo único.

Além das justificativas fornecidas no subitem 6.3, deste ETP, existem outras motivações para o agrupamento, conforme abaixo:

- Funcionamento harmônico, com compatibilidade e garantia de interligação entre todos os equipamentos e os sistemas elencados no grupo;
- Viabilidade da integração e garantia de harmonia e operacionalidade de todo o conjunto de itens adquiridos; e
- Economicidade, pois o MD ganha em capacidade de gestão do contrato, com instrumentos de cobrança efetiva e com procedimentos padronizados de suporte técnico durante o período de licenciamento e garantia, propiciando agilidade na identificação e resolução dos problemas advindos de falhas ou outros eventos que estejam relacionados ao grupo 01, que funcionarão interligados.

Em função de não haver exigência técnica de integração para as demais soluções, os itens 06, 07, 08, 09 e 10 não foram agrupados.

13. Estimativa de custo total da contratação

Valor (R\$): 10.078.170,34

A partir da composição de itens da solução, da planilha de custos e das memórias de cálculo construídas, durante a análise comparativa, para a solução escolhida, foi possível demonstrar o custo total estimado da contratação para o período de vigência do contrato de 36 meses, conforme tabela abaixo:

O valor total deverá ser pago em 3 parcelas, anuais, com data de vencimento após a assinatura do Termo de Recebimento Definitivo.

Grupo	Item	Descrição	Qtde	Valor Unitário	Valor Total
1	1	Licença de uso de software/programa de proteção de endpoints do tipo Antimalware e EDR, com instalação, configuração, suporte técnico e repasse de conhecimento.	2.400	R\$ 450,00	R\$ 1.080.000,00
	2	Licença de uso de software/programa de filtragem e proteção de navegação Web do tipo Secure Web Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	2.400	R\$ 300,00	R\$ 720.000,00
	3	Licença de uso de software/programa de prevenção de perda de dados do tipo DLP, com instalação, configuração, suporte técnico e repasse de conhecimento.	2.400	R\$ 200,00	R\$ 480.000,00

	4	Solução de prevenção e detecção de intrusão de rede do tipo IPS (Tipo I), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.10 , com instalação, configuração, suporte técnico e repasse de conhecimento.	2	R\$ 760.295,40	R\$ 1.520.590,80
	5	Solução de prevenção e detecção de intrusão de rede do tipo IPS (Tipo II), sendo o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.10 , com instalação, configuração, suporte técnico e repasse de conhecimento.	2	R\$ 312.316,32	R\$ 624.632,64
2	6	Licença de uso de software/programa de filtragem e proteção de e-mails do tipo Secure E-Mail Gateway, com instalação, configuração, suporte técnico e repasse de conhecimento.	2.150	R\$ 169,69	R\$ 364.833,50
3	7	Licença de uso de software/programa de detecção e gerenciamento de vulnerabilidades, com instalação, configuração e suporte técnico, repasse de conhecimento.	2.150	R\$ 475,87	R\$ 1.023.120,50

4	8	Solução de proteção de segurança de rede do tipo Firewall (Tipo I), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.11 , com instalação, configuração, suporte técnico e repasse de conhecimento.	4	R\$ 375.000,00	R\$ 1.500.000,00
5	9	Licença de uso de software/programa de detecção e impedimento de acesso privilegiado não autorizado a recursos críticos do tipo PAM, com instalação, configuração e suporte técnico e repasse de conhecimento.	100	R\$ 21.900,00	R\$ 2.190.000,00
6	10	Solução de proteção de segurança de rede do tipo Firewall (Tipo II), podendo ser somente a Licença de uso de software/programa ou o conjunto completo de Licença de uso de software/programa com equipamento, conforme subitem 6.11 , com instalação, configuração, suporte técnico e repasse de conhecimento.	3	R\$ 191.664,30	R\$ 574.992,90
Total					R\$ 10.078.170,34

Tabela 15

14. Justificativa técnica da escolha da solução

14.1 - Realizada a análise das duas soluções foi possível verificar que a Solução S-04 (Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança) apresentou os melhores requisitos técnicos em comparação à Solução S-05 (Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança).

14.2- Benefícios e vantagens técnicas que justificam a escolha da Solução S-04:

14.2.1 - Controle Total:

- **Personalização:** A solução licenciada oferece flexibilidade total para personalizar e configurar as ferramentas de segurança conforme as necessidades específicas do MD. As equipes da COSEC e da SC-1 terão a capacidade de ajustar parâmetros, definir políticas de segurança e personalizar fluxos de trabalho, permitindo que as ferramentas se alinhem de forma precisa aos requisitos operacionais e estratégicos da instituição. Isso garante uma adaptação contínua das soluções de segurança, sem a necessidade de customizações externas, aumentando a agilidade e a capacidade de resposta a novas demandas.
- **Independência:** Com a licença, o MD ganhará total autonomia na gestão e manutenção das ferramentas de segurança, eliminando a dependência de fornecedores ou prestadores de serviços externos. Esse nível de independência não apenas fortalece a segurança operacional, ao reduzir pontos de falha e riscos associados a acessos externos, mas também assegura maior privacidade dos dados, pois o controle das informações sensíveis fica exclusivamente dentro da instituição. As equipes da COSEC e da SC-1 poderão realizar ajustes, atualizações e modificações conforme necessário, sem sobrecarregar recursos ou depender de terceiros.
- **Integração:** A solução licenciada foi projetada para se integrar de forma eficiente com os sistemas e plataformas já em uso no MD. Com suporte para padrões abertos de integração e APIs robustas, as equipes da COSEC e da SC-1 poderão conectar as ferramentas de segurança com outros sistemas corporativos, criando um fluxo de dados coeso e automatizado. Essa facilidade de integração não só otimiza o uso das ferramentas existentes, mas também garante a continuidade dos processos operacionais com um impacto mínimo na infraestrutura já implantada, facilitando a implementação e a adaptação das soluções.

14.2.2 - Segurança:

- **Garantia de Continuidade:** A licença adquirida constitui um ativo permanente do órgão, ficando sob total controle da COSEC e da SC-1. Mesmo que, no futuro, a renovação da licença não seja viável, o software continuará em operação, embora sem acesso às atualizações e aprimoramentos oferecidos pelo fabricante. Essa continuidade minimiza os riscos relacionados à interrupção dos serviços e à perda de funcionalidade, o que não ocorre em modelos de contratação de serviços, onde, ao término do contrato ou falência da prestadora, as ferramentas de segurança seriam descontinuadas. Em um cenário de interrupção, a segurança das redes do MD estaria significativamente mais vulnerável, já que não haveria alternativas imediatas para manter as operações em andamento.
- **Menor Dependência:** A adoção da licença reduz a dependência de fornecedores externos e a exposição a riscos associados a falhas ou vulnerabilidades nos servidores de terceiros. Com a solução licenciada, a COSEC e a SC-1 manterão total controle sobre as ferramentas de segurança, o que reduz a dependência de terceiros para a gestão, manutenção e suporte. Isso fortalece a segurança operacional, pois elimina o risco de impactos devido a falhas externas, como interrupções nos serviços de nuvem, vazamentos de dados ou comprometimento de sistemas de fornecedores.

14.2.3 Conhecimento Técnico:

- **Maturidade Técnica:** A aquisição das licenças garante que a equipe da COSEC e da SC-1 mantenham o controle total sobre a administração das ferramentas de segurança, permitindo o aprimoramento contínuo do conhecimento técnico e a experiência dos profissionais responsáveis. Esse controle interno é essencial para preservar e elevar o nível de maturidade em segurança conquistado ao longo do tempo na proteção das redes ACMD e ROD. Ao gerir diretamente as ferramentas, a equipe pode adaptar as soluções de segurança de acordo com as necessidades emergentes e novas ameaças, fortalecendo a capacidade de resposta e evolução da infraestrutura de TI sem depender de fornecedores externos. Isso também assegura a continuidade do conhecimento crítico, que é vital para a manutenção da robustez e resiliência da rede a longo prazo.

14.3 - Do parcelamento da contratação decorrente de aspectos técnicos

Em que pese as soluções de segurança de TI demandadas serem autônomas, ou seja, uma solução não afeta tecnicamente a outra, as soluções que contém os itens 01, 02,

03, 04 e 05 devem funcionar de forma integrada, conforme as justificativas técnicas fornecidas no Item 6.3 e 12.2 deste ETP. Pelo exposto elas devem ser agrupadas e adquiridas do mesmo fornecedor, compondo um grupo único.

Os demais itens 06, 07, 08, 09 e 10 não precisam ser adquiridos de um único fornecedor, uma vez que não possuem interdependência entre si.

15. Justificativa econômica da escolha da solução

15.1 - Como pode ser verificado na seção 11 deste estudo - ANÁLISE COMPARATIVA DOS CUSTOS (TCO), a Equipe de Planejamento da Contratação pesquisou várias alternativas e modelos que fossem viáveis técnica e economicamente, além de adequadas às demandas deste Ministério.

15.2 - Foram analisados portais de compras do Governo Federal e atas de registro de preços contendo os itens demandados conforme as necessidades do MD, considerando quantitativos, requisitos de software e tempo de contrato.

15.3 - A solução que melhor atende às necessidades é a Solução S-04 (Contratação/Utilização das Licenças de Mercado para Ferramentas de Segurança), pois promove maior economicidade ao Ministério da Defesa entre as soluções tecnicamente viáveis, visto que o valor global para contratar a Solução S-05 (Contratação das Soluções na Forma de Serviço para Contratação/Utilização de Ferramentas de Segurança) é maior quando comparado ao período total do contrato, tanto de 12 como de 36 meses.

15.4 - Ressalta-se ainda a economia da Solução S-04 com a escolha da contratação das licenças de uso para um período de 36 meses em relação ao período de 12 meses (conforme tabela 13). Adicionalmente, é importante destacar a economia de custos indiretos resultante desta escolha de 36 meses, considerando o valor homem-hora dos profissionais do MD envolvidos na realização de processos licitatórios anuais.

15.5 - Dessa forma, a solução que melhor atendeu às necessidades econômicas foi a Solução S-04 por um período de 36 meses, a ser adquirida por meio pregão eletrônico.

15.6 - O parcelamento da contratação decorrente de aspectos econômicos

No presente caso, o agrupamento dos itens 01, 02, 03, 04 e 05, do Grupo 1 e parcelamento dos demais itens 06, 07, 08, 09 e 10, tudo da tabela 14, do item 12 deste

ETP, Descrição da Solução de TIC a Ser Contratada, decorrem de aspectos técnicos, conforme exposto no subitem 14.3 deste Estudo.

16. Benefícios a serem alcançados com a contratação

16.1 - Espera-se alcançar os seguintes benefícios, com a referida contratação:

- Identificar e registrar tráfegos e atividades suspeitas, bem como realizar os devidos bloqueios;
- Identificar vulnerabilidades em aplicações e ativos das redes de dados do MD;
- Reduzir do número de incidentes relacionados à segurança das redes de dados do MD;
- Manter níveis aceitáveis de disponibilidade, integridade, confidencialidade e integridade das informações do MD;
- Aprimorar as tecnologias de segurança de TI utilizadas nas redes de dados do MD;
- Garantir a continuidade dos negócios do MD por meio de melhorias, apoio técnico e manutenções das soluções a serem adquiridas;
- Manter as soluções com suporte e garantia dos fabricantes com por no mínimo 36 meses; e
- Manter a integração das infraestruturas, dados e sistemas das redes que compõe o MD bem como de suas redes parceiras.

17. Providências a serem Adotadas

17.1 - Providências a serem adotadas pelo MD previamente e durante à celebração do contrato:

17.1.1 - Recursos humanos:

a) Necessidade de treinamento em gestão de contratos para os servidores do Ministério, que serão designados como fiscais técnicos, administrativos e gestores, para que possam realizar suas atividades de acompanhamento e controle do contrato, conforme definido na IN nº 94/2022.

b) Necessidade de aprendizagem, por meio da transferência de conhecimento das ferramentas pela CONTRATADA, para a equipe técnica do MD, que será responsável por operar e administrar as ferramentas de segurança.

c) Técnicos da CONTRATADA com conhecimento pleno para executar ações de instalação, configuração e suporte técnico, apoiando a equipe técnica do MD na operação e administração das ferramentas de segurança.

17.1.2 - Recursos Materiais:

a) Adequação de infraestrutura de TI do MD, com a preparação e disponibilização de ambiente virtual adequado, para receber as novas ferramentas de segurança.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1 – JUSTIFICATIVA:

Conforme apresentado no subitem 12.1 deste estudo técnico, a Solução S-04 foi a que melhor atendeu às necessidades de negócio, tecnológicas e os demais requisitos para escolha da solução de TIC, previstos no item 02 deste ETP.

Cabe destacar que a solução escolhida foi a que apresentou o menor custo total estimado para o MD, conforme indicado nos itens 11.1 e 11.2.

Outro ponto relevante a ser destacado é que as desvantagens relativas à Solução S-05, listadas no item 09, são muito relevantes e tiveram importância no processo de escolha pela Solução S-04.

Conclui-se, portanto, que a opção mais adequada para prover as soluções requeridas, mitigando os riscos operacionais de continuidade dos serviços, de proteção dos dados organizacionais e com economicidade, é a Solução S-04 com validade de 36 meses. **O valor total deverá ser pago em 3 parcelas, anuais, com data de vencimento do início do contrato.**

As razões que motivaram a escolha da alternativa ou cenário, considerando as informações apuradas nas **análises técnica-funcional e econômica**:

Benefícios da Contratação alinhados ao Objetivo Estratégico 12: Aperfeiçoar a infraestrutura física e tecnológica.		
ID	Benefícios	Eficácia/ Eficiência/ Efetividade/ Economicidade
1	Identificar e registrar tráfegos e atividades suspeitas, bem como realizar os devidos bloqueios.	Eficácia
2	Identificar vulnerabilidades em aplicações e ativos das redes de dados do MD.	Eficácia
3	Reduzir do número de incidentes relacionados à segurança das redes de dados do MD.	Eficiência
4	Manter níveis aceitáveis de disponibilidade, integridade, confidencialidade e integridade das informações do MD.	Eficácia
5	Aprimorar as tecnologias de segurança de TI utilizadas nas redes de dados do MD.	Eficiência
6	Garantir a continuidade dos negócios do MD por meio de melhorias, apoio técnico e manutenções das soluções a serem adquiridas	Eficácia
7	Manter as soluções com suporte e garantia dos fabricantes com por no mínimo 36 meses	Eficácia / Economicidade
8	Manter a integração das infraestruturas, dados e sistemas das redes que compõe o MD bem como de suas redes parceiras	Eficiência

Tabela 16

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: INTEGRANTE REQUISITANTE DA DETIC

FERNANDO NOGUEIRA FILHO

Equipe de apoio



Assinou eletronicamente em 25/06/2025 às 14:12:58.

Despacho: INTEGRANTE REQUISITANTE DA SC-1

JUNIER CAMINHA AMORIM

Equipe de apoio



Assinou eletronicamente em 25/06/2025 às 20:08:19.

Despacho: INTEGRANTE TÉCNICO DA DETIC

EDMAR DA SILVA BRAGA JUNIOR

Equipe de apoio



Assinou eletronicamente em 25/06/2025 às 14:14:03.

Despacho: INTEGRANTE TÉCNICO DA SC-1

FABIO EUGENIO PRESTES BRAZ

Equipe de apoio



Assinou eletronicamente em 26/06/2025 às 09:51:07.

Despacho: AUTORIDADE MÁXIMA NA ÁREA DE TIC

BRUNO FASSHEBER NOVAIS

Autoridade competente



Assinou eletronicamente em 26/06/2025 às 14:57:02.