

INST.NAC.DE METROLOGIA QUALIDADE E TECNOLOGIA

Estudo Técnico Preliminar 14/2026**1. Informações Básicas**

Número do processo: 0052600.010616/2025-90

2. Descrição da necessidade

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base para o Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação. O ETP tem por objetivo identificar e analisar os cenários para o atendimento da demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

O presente Estudo Técnico Preliminar (ETP) decorre da necessidade formalizada no Documento de Formalização da Demanda (DFD), elaborado nos termos do Decreto nº 10.947/2022, que evidenciou a criticidade da modernização das ferramentas de segurança cibernética do órgão. O planejamento alinha-se à estratégia de transformação digital e à continuidade dos negócios, visando substituir os contratos vigentes que expiram em agosto de 2026.

2.1. Motivação

A evolução do cenário de ameaças cibernéticas, marcada pelo aumento de ataques direcionados, de códigos maliciosos do tipo *ransomware*, de exploração de vulnerabilidades críticas e de técnicas de evasão baseadas em comportamento, impõe à organização a necessidade de aprimorar seus mecanismos de proteção, detecção e resposta a incidentes de segurança da informação. Segundo alertas do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), as ameaças evoluíram de arquivos maliciosos estáticos para técnicas do tipo *fileless* (sem o uso de arquivos) e para a exploração de vulnerabilidades ainda não conhecidas ou sem correção disponível por parte dos fabricantes (*zero day*). Nesse contexto, os modelos tradicionais de proteção, com foco reativo na identificação de ameaças previamente conhecidas, mostram-se insuficientes quando utilizados isoladamente, pois não conseguem identificar adequadamente novas modalidades de ataque conduzidas por agentes maliciosos.

No âmbito do INMETRO, esse cenário é agravado pela presença de um ambiente tecnológico heterogêneo, composto por sistemas legados e estações de trabalho distribuídas, inclusive em regime de trabalho remoto, o que reduz a efetividade dos controles baseados exclusivamente no perímetro de rede. As limitações das capacidades atualmente disponíveis para proteção de e-mails, estações de trabalho e servidores corporativos resultam em uma lacuna de visibilidade sobre atividades suspeitas, especialmente em contextos em que os dispositivos operam fora da rede institucional. Nesse contexto, o Instituto não dispõe de mecanismos automatizados e integrados capazes de correlacionar eventos entre diferentes camadas de proteção e de identificar, em tempo hábil, comportamentos anômalos ou invasões em curso, independentemente da localização do ativo ou da origem da conexão.

Além disso, as subscrições das soluções atualmente utilizadas para proteger os e-mails, as estações de trabalho e os servidores de rede expiram em agosto de 2026 e apresentam limitações quanto às capacidades de análise comportamental avançada, correlação de eventos e resposta automatizada compatíveis com o cenário atual de ameaças. Conforme destacado no Documento de Formalização da Demanda (DFD), a nova contratação busca elevar o grau de automação e de eficiência da proteção, reduzir o tempo de resposta a incidentes e aumentar a resiliência

do ambiente de tecnologia da informação do Inmetro, sem necessidade de ampliação significativa da equipe técnica. Nesse contexto, a contratação deverá contemplar duas frentes complementares de fortalecimento da segurança institucional:

- Proteção do tráfego de e-mails: adoção de mecanismos avançados de inspeção, análise e mitigação de ameaças, capazes de reduzir os riscos associados a fraudes de identidade, engenharia social e códigos maliciosos distribuídos por e-mails, inclusive no contexto de coexistência com sistemas legados.
- Proteção das estações de trabalho e dos servidores de rede: evolução do modelo de proteção, incorporando capacidades de monitoramento contínuo, detecção baseada em comportamento e mecanismos automatizados de contenção de atividades suspeitas, incluindo tentativas de criptografia indevida de dados.

Alguns pontos críticos das soluções atualmente em uso que demandam adequação incluem, sem se limitar a:

- Fragmentação de Visibilidade e Limitações de Resposta (estações e servidores de rede): o modelo atualmente adotado apresenta características predominantemente reativas e pouco integradas, tratando os equipamentos de forma isolada. A ausência de uma plataforma centralizada para detecção, correlação de eventos e resposta dificulta a identificação de ataques coordenados ou de movimentos laterais que envolvam múltiplos ativos simultaneamente. Além disso, a solução vigente apresenta limitações quanto aos recursos de remediação remota e de contenção automatizada, o que exige intervenções manuais da equipe técnica e contribui para o aumento do tempo de resposta e da exposição a incidentes de segurança.
- Limitações na Proteção contra Engenharia Social (E-mail): a solução de proteção de e-mail atualmente adotada apresenta limitações na detecção de ataques de *phishing* direcionado (*spear phishing*) e de fraudes de comprometimento de e-mail corporativo (*Business Email Compromise – BEC*), que não se baseiam em anexos maliciosos tradicionais. A solução atual também não contempla mecanismos estruturados de revisão e neutralização de mensagens após a entrega, nem recursos de inspeção dinâmica de URLs no momento da interação do usuário, o que dificulta a mitigação de links que se tornam maliciosos após o recebimento da mensagem. Tais limitações reduzem a capacidade institucional de responder a técnicas modernas de engenharia social e aumentam o risco de comprometimento de informações institucionais, especialmente diante de estratégias que exploram variações de domínio, falsificação de identidade e mudanças dinâmicas de conteúdo.
- Riscos Relacionados à Conformidade Normativa: As limitações técnicas atualmente identificadas podem restringir a capacidade institucional de atender integralmente aos requisitos estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), especialmente no que se refere à rastreabilidade de incidentes, à preservação de evidências e à comunicação tempestiva de incidentes de segurança. Adicionalmente, a ausência de mecanismos avançados de registro, correlação e auditoria pode dificultar o fortalecimento dos controles exigidos pelas normas expedidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e pelas diretrizes do Programa de Privacidade e Segurança da Informação, conduzido pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), o que demanda aprimoramento da capacidade de monitoramento e de resposta a incidentes.
- Limitações na Gestão, Visibilidade e Resposta em Ambiente Distribuído: A ampliação do trabalho remoto e híbrido, aliada à diversidade de estações de trabalho e de servidores que compõem o ambiente institucional, impõe desafios adicionais à gestão centralizada da segurança dos dispositivos, especialmente quando estes operam fora do perímetro tradicional da rede. O modelo atualmente adotado apresenta limitações quanto à verificação contínua da conformidade dos agentes de proteção, à aplicação uniforme de políticas de segurança e à atualização tempestiva dos mecanismos de defesa em equipamentos que não permanecem conectados à rede corporativa. Adicionalmente, a inexistência de mecanismos integrados que permitam o monitoramento contínuo, a correlação de eventos entre ativos distintos e ações coordenadas de contenção dificulta a identificação precoce de comportamentos anômalos e pode ampliar o impacto operacional de incidentes de segurança.

Considerando a complexidade técnica envolvida na migração e na coexistência de aproximadamente 1.900 estações de trabalho e servidores de rede (*endpoints*) e de 2.600 contas de e-mail em ambiente heterogêneo, o trâmite licitatório deverá observar o princípio da continuidade do serviço público. A transição para soluções modernas de proteção de *endpoints* e de e-mail demandará planejamento estruturado de homologação, implantação gradual e repasse de conhecimento à equipe técnica. Dessa forma, recomenda-se a instauração do processo licitatório em

tempo hábil, de modo a assegurar que os mecanismos de proteção institucional e a integridade das informações permaneçam adequadamente preservados antes da expiração das subscrições vigentes, prevista para agosto de 2026.

A presente contratação encontra-se alinhada aos seguintes instrumentos de planejamento institucional:

- Plano Estratégico do Inmetro 2024–2027 – Objetivo Estratégico 15: Aprofundar a transformação digital com foco na integração e portabilidade de sistemas;
- Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) 2025–2027 – Necessidade de Infra NINFRA4 – Infraestrutura de Segurança da Informação, Meta M4: Adquirir ou renovar soluções de proteção de endpoints e de e-mail.

2.2 Justificativa da necessidade da contratação

A presente contratação fundamenta-se na necessidade de adequação das ferramentas de segurança para proteção de endpoints e de e-mails atualmente em operação, na iminência do término das subscrições vigentes em agosto de 2026 e na necessidade estratégica de otimizar a força de trabalho da equipe técnica interna. O atual cenário de ameaças cibernéticas exige a transição de um modelo de segurança passivo e reativo para um ecossistema automatizado e resiliente, capaz de correlacionar eventos e responder a incidentes em tempo real, sem a necessidade de intervenções manuais exaustivas.

1) Proteção de Endpoints (Endpoint Detection and Response - EDR): A solução vigente opera sob uma lógica predominantemente preventiva, mostrando-se ineficaz na detecção comportamental e na investigação forense necessárias no atual cenário de ataques fileless e de movimentações laterais de ransomware. A ausência de capacidade de Endpoint Detection and Response (EDR) cria uma "lacuna de visibilidade" que impede a administração de identificar e conter ameaças avançadas que já tenham contornado as defesas de borda, expondo o parque tecnológico do Inmetro a paralisias operacionais e ao sequestro de dados sensíveis.

2) Proteção de Correio Eletrônico (*Secure E-mail Gateway* – SEG): O gateway de e-mail atualmente em uso apresenta limitações funcionais e tecnológicas diante do cenário atual de ameaças, especialmente na identificação de ataques de engenharia social (como spear phishing e BEC), o que pode impactar a eficácia dos mecanismos de proteção e a governança do órgão, tais como:

- Obsolescência e Insegurança de Software: Impossibilidade técnica de atualizar a solução para versões suportadas pelo fabricante, mantendo o serviço exposto a vulnerabilidades conhecidas e sem correções de segurança;
- Incompatibilidade com a Infraestrutura Institucional: Falta de aderência com ambientes baseados em Linux e dificuldade de integração com diretórios LDAP/LDAPS, elementos centrais da topologia de rede do Inmetro, o que gera falhas de sincronização e lacunas na aplicação de políticas;
- Déficit de Governança e Segregação de Funções: Interface administrativa inadequada que impede a gestão granular de perfis (RBAC - *Role-Based Access Control*), impossibilitando a auditoria de ações e o cumprimento de boas práticas de governança de TI;
- Ineficiência Operacional: A baixa eficácia de filtragem resulta em um volume excessivo de ameaças chegando às caixas postais de 2.600 contas, exigindo que a equipe de TIC despenda esforço desproporcional em tarefas manuais de remediação e de suporte aos usuários.

A manutenção do *status quo* eleva exponencialmente o risco de exfiltração de dados e de interrupção de serviços críticos. A substituição por soluções de nova geração não é apenas uma atualização tecnológica, mas também uma medida mandatória para alinhar o Inmetro aos controles de segurança exigidos pela Secretaria de Governo Digital (SGD) e pelo Gabinete de Segurança Institucional (GSI/PR), garantindo a integridade dos ativos digitais e a eficiência na gestão dos recursos públicos.

A presente contratação pretende adquirir subscrições de licenças de software de segurança da informação, contemplando as Soluções de Detecção e Resposta em Endpoint (EDR) e de Proteção Avançada de Correio Eletrônico (Secure Email Gateway - SEG), incluindo suporte técnico, atualização e garantia por 36 (trinta e seis) meses, da seguinte forma:

ITEM	DESCRIÇÃO
1	Proteção de Endpoints (<i>Endpoint Detection and Response</i> -EDR)
2	Proteção de Correio Eletrônico (<i>Secure E-mail Gateway</i> – SEG)

3. Área requisitante

Área Requisitante	Responsável
PRESI/CTINF/DIINF	Paulo Gustavo de Oliveira Del Peloso

4. Necessidades de Negócio

As necessidades de negócio, também denominadas requisitos de negócio, conforme as diretrizes do Guia BABOK (*Business Analysis Body of Knowledge*), representam os objetivos de alto nível, as metas estratégicas e as lacunas organizacionais que motivam a realização desta iniciativa. Estas necessidades descrevem as razões que justificam o investimento, os resultados esperados para a organização e os benefícios a serem alcançados com a modernização tecnológica proposta.

Nesse contexto, esta seção identifica e descreve as necessidades que fundamentam a contratação de soluções de Proteção de Endpoints (EDR) e de Proteção de Correio Eletrônico (SEG), as quais orientam a análise de alternativas e a definição da solução mais aderente aos objetivos institucionais do Inmetro.

4.1. Necessidades de Negócio Comuns aos dois Itens

4.1.1. Fortalecimento da Resiliência Cibernética e da Continuidade de Negócio. Diante da sofisticação dos ataques globais, torna-se essencial fortalecer os mecanismos de proteção do ecossistema tecnológico do Inmetro. A necessidade primária é reduzir o risco de incidentes que comprometam a tríade da segurança (confidencialidade, integridade e disponibilidade), garantindo que os serviços prestados à sociedade não sofram interrupções por ataques de sequestro de dados (*Ransomware*) ou por sabotagem digital.

4.1.2. Ampliação da Capacidade de Detecção e de Resposta Automatizada. As ferramentas atuais não oferecem o nível de inteligência necessário para enfrentar ameaças modernas em tempo real. Há uma necessidade crítica de reduzir o tempo de resposta aos incidentes, automatizando a contenção de ameaças, inclusive fora do horário comercial, minimizando a janela de exposição a riscos e limitando o impacto de possíveis invasões.

4.1.3. Aprimoramento da Governança, da Visibilidade e do Compliance. A adoção de soluções de nova geração deve proporcionar visibilidade centralizada sobre eventos e tendências de ameaças em todo o parque tecnológico. Essa necessidade visa apoiar a tomada de decisão baseada em dados e assegurar o cumprimento de normas legais e regulatórias, facilitando auditorias e investigações forenses.

4.1.4. Mitigação de Riscos de Exfiltração de Dados e de Danos Reputacionais. É imperativo prevenir o vazamento de informações sensíveis e a exfiltração de dados institucionais que comprometam a propriedade intelectual ou a privacidade de terceiros. Além da perda financeira, a contratação visa proteger a reputação digital do Inmetro, evitando que seus domínios e IPs sejam listados em blacklists internacionais, o que prejudicaria a comunicação oficial e a credibilidade do Instituto.

4.1.5. Otimização da Eficiência Operacional da Equipe Técnica. Considerando a limitação de recursos humanos especializados, o negócio demanda soluções que reduzam a dependência de processos manuais exaustivos. A automação das ferramentas de EDR e SEG deve permitir que a equipe técnica atue de forma estratégica na gestão de riscos e na melhoria contínua do ambiente, em vez de desperdiçar esforços em manutenção de softwares obsoletos e em remediações repetitivas.

4.1.6 Proteção Preventiva Contra Ameaças de Dia Zero (Zero Day). Dada a obsolescência das atuais proteções, é necessária a implementação de tecnologias de análise comportamental e de Sandbox capazes de identificar e bloquear ataques inéditos. O foco é evitar a paralisia das atividades finalísticas do Inmetro decorrente de vulnerabilidades para as quais ainda não existem correções oficiais dos fabricantes.

4.1.7 Capacidade potencial ou futura de integração com ambientes de nuvem. Garantir que as soluções possuam a capacidade de evolução tecnológica para suportar futuras arquiteturas híbridas ou em nuvem, evitando substituições prematuras da solução de segurança.

4.2. Necessidades de Negócio Específicas – Item 1: Proteção de Endpoints (EDR)

4.2.1. Detecção de Inteligência Comportamental e Ameaças Invisíveis. Os endpoints (estações de trabalho e servidores) representam a última linha de defesa e um dos principais alvos de ataques modernos. Existe a necessidade crítica de uma solução que transcenda a simples detecção por assinaturas, capaz de identificar comportamentos anômalos, atividades de movimento lateral e ataques fileless (sem arquivo) em tempo real. A inteligência da ferramenta deve permitir correlacionar eventos isolados para detectar invasões complexas que buscam burlar os mecanismos tradicionais de proteção.

4.2.2. Resposta Orquestrada e Contenção Remota de Incidentes. É imperativo dispor de mecanismos que permitam uma resposta centralizada e imediata a incidentes, sem a necessidade de deslocamento físico da equipe técnica até o ativo comprometido. A necessidade de negócio foca na capacidade de realizar o isolamento lógico de máquinas infectadas, a interrupção de processos maliciosos e remediação remota em larga escala (cerca de 1.900 ativos). Adicionalmente, torna-se essencial a disponibilização de acesso remoto seguro e integrado aos endpoints, permitindo a investigação e a execução de ações corretivas em tempo real, com registro auditável das atividades realizadas. O objetivo é reduzir drasticamente o tempo de contenção, evitando que uma infecção local se transforme em um incidente sistêmico de grande proporção, bem como apoiar a análise e a tomada de decisão por meio de recursos avançados que auxiliem na interpretação de eventos e na recomendação de ações de resposta e remediação, contribuindo para maior eficiência operacional.

4.2.3. Visibilidade Forense e Análise de Causa Raiz. A instituição demanda visibilidade consolidada e histórica sobre a saúde e segurança de todos os seus ativos. Mais do que apenas bloquear uma ameaça, o negócio precisa entender a "linhagem" do ataque: como ele entrou, quais arquivos modificou e quais comunicações tentou estabelecer. Essa capacidade de investigação forense digital é essencial para apoiar a tomada de decisões estratégicas de segurança, permitindo o fechamento de brechas estruturais e o aprimoramento contínuo das políticas de defesa do Inmetro.

4.3. Necessidades de Negócio Específicas – Item 2: Proteção de Correio Eletrônico (SEG)

4.3.1. Proteção Contra Ameaças Avançadas e Engenharia Social (BEC/Phishing). Mitigar o risco de interrupção das atividades e de prejuízo ao erário decorrentes de ataques modernos. O e-mail é o principal vetor de *ransomware* e de fraudes financeiras (BEC). A solução deve identificar ameaças que não utilizam arquivos maliciosos (como golpes de falsidade ideológica contra a alta gestão), protegendo perfis de usuários críticos e permitindo ações educativas baseadas no comportamento de risco detectado.

4.3.2. Proteção e Resiliência de Ambientes Legados e Heterogêneos. Garantir a continuidade e segurança das comunicações oficiais em um cenário técnico complexo. A solução deve atuar como uma camada de proteção externa ("*shielding*") para sistemas que não recebem mais atualizações de segurança (como o Microsoft Exchange 2010) e plataformas distintas (como o Zimbra), unificando a gestão de segurança. Deve operar de forma resiliente, com alta disponibilidade, na infraestrutura de virtualização atual (VMware 6.5), sem criar novas vulnerabilidades nos servidores de diretório (integração sem agentes).

4.3.3. Autonomia do Usuário e Gestão de Contas Compartilhadas. Existe a necessidade estratégica de conferir autonomia aos usuários finais na gestão de suas mensagens retidas, especialmente em contas de e-mail departamentais ou compartilhadas que não possuem credenciais de acesso direto a portais web. A solução deve permitir a tomada de decisões de segurança (liberação, bloqueio e reporte) de forma ágil, diretamente a partir de notificações enviadas para a própria caixa postal, reduzindo o volume de chamados de suporte técnico e garantindo a continuidade dos processos de negócio que dependem dessas comunicações.

4.3.4. Sustentabilidade e Transição para Arquiteturas Híbridas. Garantir que o investimento seja duradouro e suporte a evolução tecnológica da instituição. A solução deve permitir a convivência e a migração gradual entre ambientes *on-premises* e na nuvem (Microsoft 365/Google Workspace), protegendo múltiplos domínios por meio de um console centralizado. Isso evita a fragmentação das políticas de segurança e reduz o custo operacional de gestão (TCO) ao tratar fluxos de entrada e de saída em uma única plataforma.

5. Necessidades Tecnológicas

As necessidades tecnológicas, também denominadas requisitos da solução, conforme as diretrizes do Guia BABOK (*Business Analysis Body of Knowledge*), descrevem as capacidades, qualidades e características técnicas indispensáveis que as ferramentas devem possuir para o pleno atendimento aos objetivos de negócio do Inmetro.

Diferentemente das metas estratégicas de alto nível, estas necessidades traduzem os requisitos funcionais e não funcionais em especificações de arquitetura, segurança e interoperabilidade. Elas foram definidas a partir de uma análise técnica detalhada do ambiente institucional, marcado pela presença de sistemas heterogêneos e legados, e do cenário atual de ameaças cibernéticas, assegurando que as soluções selecionadas sejam tecnicamente capazes de proporcionar a proteção e a automação desejadas, sem comprometer a estabilidade da infraestrutura existente.

As necessidades tecnológicas detalhadas abaixo orientarão a elaboração das especificações técnicas do Termo de Referência (TR), servindo como critérios de conformidade e seleção no processo licitatório.

5.1. Necessidades Tecnológicas Comuns aos Dois Itens

5.1.1. Gerenciamento Centralizado e Interface Gráfica (GUI) via HTTPS. As soluções devem prover consoles de gerenciamento centralizados, acessíveis via protocolo seguro (HTTPS), que permitam a configuração, o monitoramento e a resposta a incidentes de forma unificada para todo o parque tecnológico. Essa necessidade tecnológica visa eliminar a complexidade operacional, garantindo que a equipe técnica tenha uma visão clara do estado de segurança de 1.900 endpoints e 2.600 contas de e-mail, sem a necessidade de comandos em linha de texto ou edições manuais de arquivos de configuração, otimizando o tempo de resposta e a curva de aprendizado.

5.1.2. Governança de Acesso e Segregação de Funções (RBAC). As plataformas devem suportar nativamente o controle de acesso baseado em perfis (Role-Based Access Control - RBAC), permitindo a definição granular de permissões para diferentes administradores e técnicos. Essa funcionalidade tecnológica é essencial para o cumprimento das normas de governança e auditoria do Inmetro, garantindo a segregação de funções, a rastreabilidade completa de todas as alterações de configuração e das ações de resposta realizadas nas ferramentas, e mitigando riscos de erros humanos ou acessos administrativos indevidos.

5.1.3. Alta Disponibilidade, Escalabilidade e Resiliência Operacional. As arquiteturas tecnológicas propostas devem ser projetadas para garantir alta disponibilidade dos serviços, com suporte a modelos de redundância e recuperação de falhas (failover) que assegurem a continuidade ininterrupta da proteção. Dado o volume de dados e o crescimento projetado da infraestrutura, as soluções devem ser escaláveis para suportar o aumento do tráfego de e-mails e a adição de novos ativos de rede, mantendo o desempenho e a eficácia da detecção mesmo sob condições de carga elevada.

5.1.4. Capacidade de Auditoria e Integração com Sistemas de Logs (Syslog/SIEM). As soluções devem possuir mecanismos robustos de geração de logs detalhados e relatórios analíticos, com suporte à exportação de eventos via protocolos padrão (ex: Syslog). Essa necessidade tecnológica visa garantir que todos os incidentes de segurança e as ações administrativas sejam registrados e correlacionados com ferramentas externas de monitoramento (SIEM) ou de auditoria.

5.1.5. Capacidade de Evolução para Ambientes de Computação em Nuvem. Embora a infraestrutura tecnológica atual da instituição esteja predominantemente baseada em servidores e serviços locais (on-premises), observa-se uma tendência crescente de adoção gradual de serviços de computação em nuvem em organizações públicas e privadas, especialmente para hospedagem de aplicações, ambientes de desenvolvimento, serviços de colaboração e soluções de análise de dados. Nesse contexto, torna-se recomendável que as soluções possuam capacidade básica de integração ou compatibilidade com ambientes de nuvem pública, permitindo a identificação e proteção de serviços e ativos eventualmente instanciados em plataformas como Microsoft Azure ou Amazon Web Services (AWS). Essa característica não implica a adoção imediata de infraestrutura em nuvem pela instituição, mas busca garantir que a solução selecionada esteja preparada para suportar cenários híbridos no futuro, evitando a necessidade de substituição prematura da tecnologia de segurança caso haja expansão da infraestrutura em nuvem. Dessa forma, preserva-se a sustentabilidade da solução ao longo de seu ciclo de vida e assegura-se maior flexibilidade para a evolução da arquitetura de TI institucional.

5.2. Necessidades Tecnológicas Específicas – Item 1: Proteção de Endpoints (EDR)

5.2.1. Arquitetura de Agente Único e Cobertura Multiplataforma. A solução tecnológica deve ser baseada em um agente único, que integre nativamente as capacidades de prevenção (EPP) e detecção/resposta (EDR), evitando a sobrecarga de processamento nos ativos. É imperativo que a tecnologia suporte, de forma unificada, os sistemas operacionais Windows, Linux e macOS, permitindo o gerenciamento e a proteção contínua de notebooks e servidores, tanto dentro quanto fora da rede institucional, garantindo a visibilidade total do parque de endpoints, independentemente de sua localização geográfica ou de sua conectividade ao domínio local.

5.2.2. Capacidade de Detecção Comportamental e Correlação de Eventos. A tecnologia deve possuir motores de inteligência artificial e de análise comportamental capazes de identificar ameaças avançadas, como ataques fileless (sem arquivo), execuções em memória e o uso malicioso de scripts legítimos que burlam assinaturas estáticas. A necessidade tecnológica foca na capacidade do EDR de correlacionar, de forma agregada, eventos anômalos entre diversos ativos, permitindo à equipe de TI visualizar a linhagem completa de um incidente e identificar tentativas de movimento lateral antes que ocorra o comprometimento sistêmico dos dados institucionais.

5.2.3. A solução deve oferecer capacidades de resposta rápida e orquestrada, permitindo ações automatizadas ou assistidas pela equipe técnica para a contenção imediata de ameaças. Isso inclui, obrigatoriamente, funcionalidades como o isolamento lógico do *endpoint* na rede, a interrupção de processos suspeitos, o bloqueio de atividades maliciosas e a remediação de alterações indevidas no sistema operacional. A tecnologia deverá ser capaz de detectar comportamentos anômalos associados a ameaças avançadas, incluindo tentativas de criptografia maliciosa típicas de *ransomware*, permitindo sua interrupção automática e a recuperação das alterações causadas. Essa capacidade tecnológica é essencial para reduzir o tempo de resposta a incidentes de segurança e mitigar o impacto operacional de ataques, possibilitando que a contenção e a remediação sejam realizadas remotamente por meio de console centralizado, sem necessidade de intervenção física nos ativos afetados.

5.2.4. Gestão Centralizada e Distribuição Automatizada de Agentes. A administração de todo o ecossistema de segurança de *endpoints* deve ser realizada por meio de um console único e intuitivo, que ofereça visibilidade em tempo real sobre o inventário, o estado de conformidade e os alertas de segurança dos ativos. A solução tecnológica deve permitir a distribuição, instalação e atualização dos agentes de forma automatizada e em larga escala, com mecanismos próprios de entrega ou integração com ferramentas de *deployment* existentes, de modo a assegurar a cobertura total do parque tecnológico com o mínimo esforço operacional e de intervenção manual da equipe de TI.

5.2.5. Proteção Avançada contra Ransomware e Explorações. A solução tecnológica deve incorporar mecanismos específicos de proteção contra *ransomware* e técnicas modernas de exploração, indo além da detecção tradicional baseada em assinatura. É imperativo que a plataforma possua capacidade de identificar comportamentos típicos de criptografia maliciosa em tempo real, bloqueando automaticamente o processo ofensivo antes de sua conclusão. Adicionalmente, a tecnologia deve contemplar funcionalidade de reversão de alterações indevidas (*rollback*), permitindo restaurar arquivos impactados por criptografia não autorizada, quando tecnicamente viável. A solução deve ainda incluir mecanismos de mitigação de *exploits*, com proteção contra execução de código em memória, elevação indevida de privilégios e exploração de vulnerabilidades conhecidas ou desconhecidas (*zero-day*), reduzindo significativamente a superfície de ataque dos ativos institucionais. Essa necessidade tecnológica decorre do aumento exponencial de ataques direcionados a organizações públicas, cujo impacto pode comprometer a continuidade de serviços essenciais.

5.2.6. Capacidade de Investigação Avançada e de Threat Hunting. A solução deve disponibilizar recursos avançados de investigação e de busca ativa por ameaças (*threat hunting*), permitindo à equipe técnica realizar consultas detalhadas sobre eventos, indicadores de comprometimento (IOCs), processos executados, conexões de rede e alterações sistêmicas nos *endpoints* protegidos. É importante a manutenção de um repositório centralizado de telemetria, com retenção histórica adequada, que permita análises retroativas e investigações forenses, mesmo após a mitigação inicial do incidente. A tecnologia deve permitir a execução de consultas estruturadas e filtradas, com capacidade de correlação temporal e entre múltiplos ativos, apoiando a identificação de movimentos laterais e de campanhas coordenadas. Tal funcionalidade é essencial para elevar o nível de maturidade da postura defensiva institucional, permitindo uma atuação proativa, e não apenas reativa, diante de ameaças sofisticadas.

5.2.7. Controle de Aplicações e Dispositivos. A solução tecnológica deve oferecer mecanismos integrados de controle de aplicações (*application control*) e de dispositivos externos (*device control*), funcionalidades existentes na atual solução em uso, permitindo estabelecer políticas restritivas ou permissivas com base em critérios como *hash* do arquivo, editor confiável, categoria de software ou grupo de usuários. No tocante ao controle de dispositivos removíveis, a solução deve possibilitar o gerenciamento do uso de mídias USB, de dispositivos de armazenamento externo e de interfaces de comunicação, com capacidade de bloqueio, liberação controlada ou monitoramento de atividades. Deve ainda permitir a definição de políticas diferenciadas por perfil de usuário ou por unidade organizacional. Essa necessidade tecnológica visa reduzir riscos associados à introdução de malware por meio de mídias externas e à exfiltração não autorizada de dados institucionais, fortalecendo os mecanismos de prevenção internos.

5.2.8. Prevenção da exfiltração de dados. A solução deve contemplar recursos de prevenção à perda de dados integrados à proteção de *endpoints*, permitindo identificar, monitorar e controlar a movimentação de informações sensíveis armazenadas ou manipuladas nos ativos institucionais. Essa funcionalidade tecnológica é indispensável para mitigar riscos de vazamento de informações e assegurar conformidade com a Lei Geral de Proteção de Dados Pessoais, fortalecendo a governança de dados no âmbito institucional.

As capacidades tecnológicas descritas nesta seção representam os requisitos mínimos necessários para atendimento ao nível de risco institucional identificado, devendo ser refletidas nos requisitos técnicos do Termo de Referência correspondente.

5.3. Necessidades Tecnológicas Específicas – Item 2: Proteção de Correio Eletrônico (SEG)

5.3.1. Arquitetura de Appliance Virtual e Compatibilidade com Hypervisors. A solução deve ser disponibilizada obrigatoriamente em formato de *appliance* virtual dedicado para execução local (*on-premise*). É imperativo que a plataforma suporte nativamente o hypervisor VMware ESXi 6.5 ou superior, permitindo a implantação imediata sem a necessidade de atualizações onerosas ou arriscadas na camada de virtualização existente.

5.3.2. Capacidade de Gateway SMTP para Ambientes Heterogêneos e Legados. Devido à coexistência de diferentes plataformas de correio eletrônico (Microsoft Exchange 2010 e Zimbra 8.x), a tecnologia deve operar obrigatoriamente como um *Mail Transfer Agent* (MTA) ou Gateway SMTP agnóstico. Essa capacidade permite que a filtragem ocorra de forma transparente e centralizada para todos os fluxos de e-mail, assegurando a proteção de sistemas legados que não têm mais suporte oficial de segurança contra vulnerabilidades conhecidas.

5.3.3. Mecanismos de Detecção Avançada, Sandbox e Inteligência de Ameaças. A solução deve integrar tecnologias de análise dinâmica em ambiente controlado (Sandbox) para detecção de ameaças de dia zero (*zero-day*), além de motores de inteligência artificial voltados à mitigação de ataques de *Business Email Compromise* (BEC) e de fraudes de personificação. Complementarmente, deve possuir capacidade de inspeção de vetores modernos de ataque, como a extração e análise de URLs de códigos QR e a reescrita de links (*URL Sandboxing*), garantindo proteção contínua mesmo após a entrega da mensagem.

5.3.4. Análise Temática e Contextual de BEC. A solução deve possuir capacidade analítica para classificar as tentativas de ataque de Business Email Compromise (BEC) por temas ou táticas (ex.: fraude de faturas, redirecionamento de folha de pagamento, solicitações de cartões-presente, entre outros). Essa visibilidade deve permitir a identificação de tendências de ataques direcionados a departamentos específicos e usuários críticos, apoiando a tomada de decisão para treinamentos de conscientização focados.

5.3.5. Alta Disponibilidade Ativo-Ativo e Gestão Centralizada de Quarentena. A arquitetura tecnológica deve suportar operação em cluster de alta disponibilidade no modo ativo-ativo, com sincronização automática de configurações e *failover* transparente para garantir a continuidade ininterrupta do serviço. Toda a administração de políticas em múltiplos domínios, bem como a gestão de quarentenas individualizadas para os usuários finais, deve ser centralizada em uma única interface gráfica (GUI), o que simplifica a operação e reduz o esforço administrativo das equipes de TI e de suporte.

As capacidades tecnológicas descritas nesta seção representam os requisitos mínimos necessários para atendimento ao nível de risco institucional identificado, devendo ser refletidas nos requisitos técnicos do Termo de Referência correspondente.

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

Esta seção detalha as condições essenciais de arquitetura, licenciamento e prestação de serviços a serem observadas para garantir o alcance dos objetivos estratégicos e a plena operacionalização das soluções de EDR e SEG no ambiente institucional.

6.1. Requisitos Gerais (comuns aos itens 1 e 2)

6.1.1. Arquitetura Adaptativa e Gestão de Ativos Remotos. As soluções devem garantir o monitoramento, a visibilidade e a proteção contínua de todos os ativos da Instituição, independentemente de sua localização física ou da forma de conexão à rede (local, remota ou em trânsito). É imperativo que a tecnologia permita o gerenciamento de incidentes e a aplicação de políticas em tempo real para todos os equipamentos e contas de e-mail, assegurando a proteção integral de usuários em regime de teletrabalho ou mobilidade, sem que a eficácia da detecção ou a agilidade da resposta dependam exclusivamente de infraestruturas de conexão privada (VPN).

6.1.2. Modelo de Subscrição, Atualização e Suporte Técnico 24x7. As soluções serão adquiridas sob o modelo de subscrição, pelo período de 36 (trinta e seis) meses, com pagamento condicionado à entrega e à aceitação definitivas. A subscrição deve contemplar o direito de uso integral, atualizações de versão, atualizações contínuas das assinaturas de ameaças e suporte técnico direto do fabricante, em regime de 24 horas por dia, 7 dias por semana (24x7), com canais de atendimento que assegurem o suporte a incidentes críticos.

6.1.3. Implementação Técnica, Calibragem e Operação Assistida. A CONTRATADA será responsável pela instalação completa das soluções e pela configuração das políticas de segurança, incluindo o processo de tuning (refinamento) para reduzir falsos positivos no ambiente institucional. O escopo deve incluir a fase de "operação assistida" e hands-on, garantindo que a transição para a produção ocorra de forma segura e que haja o efetivo repasse de conhecimento técnico à equipe do Inmetro, capacitando-a para a gestão autônoma das plataformas de EDR e SEG.

6.1.4. Interoperabilidade, Governança e Rastreabilidade das Ações. As soluções devem ser plenamente compatíveis com o ecossistema tecnológico existente (especialmente com sistemas operacionais Linux/Windows e diretórios LDAP), permitindo a administração centralizada por meio de interfaces intuitivas. É imperativo que as ferramentas ofereçam mecanismos robustos de auditoria, registrando todas as ações administrativas e as alterações de política, para fins de rastreabilidade forense e de conformidade com as boas práticas de segurança da informação.

6.1.5. Documentação Técnica e Atualização Contínua de Mecanismos. É obrigatória a entrega da documentação técnica completa e dos manuais de operação em português ou inglês. A solução deve demonstrar capacidade de atualização contínua e autônoma de seus mecanismos de proteção contra novas variantes de ameaças, assegurando que o Inmetro permaneça protegido contra vulnerabilidades emergentes durante todo o período de vigência contratual.

6.2. Requisitos Específicos – Item 1: Proteção de Endpoints (EDR)

Este item contempla a aquisição de uma plataforma de proteção de última geração para 1.900 ativos (estações de trabalho e servidores), visando à substituição do modelo preventivo tradicional de proteção de endpoint por uma arquitetura de monitoramento ativo e contínuo em plataformas Windows, Linux e macOS. A necessidade tecnológica foca na implementação de capacidades de Detecção e Resposta (EDR) assistidas por Inteligência Artificial, capazes de identificar comportamentos maliciosos e ataques fileless que burlam assinaturas estáticas. O objetivo central é

dotar o Inmetro de visibilidade total sobre o seu parque tecnológico, permitindo a contenção imediata de ameaças por meio de isolamento remoto e a investigação forense de incidentes a partir de um console unificado, reduzindo drasticamente o tempo de resposta (MTTR) e a necessidade de intervenções físicas nos ativos.

As especificações técnicas detalhadas, as capacidades mandatórias de detecção e resposta, bem como os requisitos de gerenciamento deste item, encontram-se descritos no ANEXO I – Especificação Técnica: Proteção de Endpoints (EDR) deste documento.

6.3. Requisitos Específicos – Item 2: Proteção de Correio Eletrônico (SEG)

Este item contempla a implementação de uma solução de gateway de segurança de correio eletrônico (Secure Email Gateway - SEG) em arquitetura on-premise, visando a proteção de 2.600 contas de e-mail operadas em ambientes heterogêneos (Microsoft Exchange 2010 e Zimbra 8.x). A necessidade foca na substituição da ferramenta atual, considerada obsoleta, por uma plataforma de inteligência cibernética capaz de mitigar ataques sofisticados de Business Email Compromise (BEC), Spear Phishing e fraudes de personificação que não exigem anexos maliciosos. O objetivo central é prover uma blindagem ativa para os servidores legados por meio de tecnologias, por exemplo, de Sandbox, análise dinâmica de URLs (Time-of-Click) e inspeção de códigos QR (QR Code).

As especificações técnicas detalhadas, as capacidades mandatórias de filtragem, proteção avançada e os requisitos de gerenciamento deste item, encontram-se descritos no ANEXO II – Especificação Técnica: Proteção de Correio Eletrônico (SEG) deste documento.

7. Estimativa da demanda - quantidade de bens e serviços

Esta seção registra, de forma detalhada e motivada, o quantitativo estimado de bens e serviços necessários à composição da solução, conforme os preceitos da IN SGD/ME nº 94/2022. A estimativa baseia-se no Documento de Formalização de Demanda (DFD) e no inventário atual do ambiente tecnológico do Inmetro, visando garantir a continuidade operacional, sem interrupções, após o término das subscrições vigentes em agosto de 2026. Eventuais ajustes nos quantitativos poderão ser realizados na fase de elaboração do Termo de Referência, com base na atualização do inventário institucional.

7.1 Item 1: Proteção de Endpoints (EDR)

A demanda foi calculada para assegurar a proteção integral do parque computacional do Inmetro, incluindo as estações de trabalho e os servidores.

Quantidade Estimada: 1.905 (mil novecentas e cinco) subscrições.

Período de Cobertura: 36 (trinta e seis) meses.

Memória de Cálculo e Justificativa: O quantitativo reflete o inventário consolidado de ativos (estações de trabalho e servidores) a serem protegidos pela solução, distribuído conforme segue: (a) 350 (trezentas e cinquenta) estações de trabalho com Windows 7 ou superior; (b) 1.450 (mil quatrocentas e cinquenta) estações de trabalho com Windows 10 ou superior; (c) 30 (trinta) servidores com Windows Server 2008 R2 ou Windows Server 2012 R2; (d) 75 (setenta e cinco) servidores com Windows Server 2016 ou superior.

A estimativa visa à substituição integral do modelo de licenciamento atual, sem ampliação de escopo, garantindo que nenhum ativo institucional permaneça desprotegido durante a transição tecnológica;

O número baseia-se no contrato vigente, iniciado em outubro de 2023, e considera o montante mínimo necessário à manutenção da resiliência do parque tecnológico.

7.2 Item 2: Proteção de Correio Eletrônico (SEG)

A demanda foi dimensionada para prover a blindagem do serviço de correio eletrônico institucional (Zimbra e Exchange), protegendo a comunicação oficial de todas as unidades do órgão.

Quantidade Estimada: 2.675 (duas mil seiscentas e setenta e cinco) licenças de contas de e-mail.

Período de Cobertura: 36 (trinta e seis) meses.

Memória de Cálculo e Justificativa: O quantitativo foi definido com base no número atual de caixas postais ativas nos servidores institucionais;

A estimativa contempla a proteção de todos os domínios oficiais e a filtragem de fluxos de entrada e saída (inbound /outbound);

O licenciamento assegura a cobertura integral do serviço durante toda a vigência contratual de 36 meses, permitindo a migração e a convivência entre as plataformas legadas e futuras sem lacunas de proteção.

8. Levantamento de soluções

O levantamento de soluções fundamenta-se na identificação e análise de alternativas tecnicamente viáveis e disponíveis no mercado para atender à demanda formalizada no DFD. O objetivo primordial é selecionar tecnologias que ofereçam o melhor equilíbrio entre eficácia defensiva, custo-benefício e aderência à infraestrutura institucional, observando rigorosamente as diretrizes da Instrução Normativa SGD/ME nº 94/2022.

Para tanto, foram consideradas soluções amplamente adotadas no mercado e na Administração Pública, observando-se, entre outros aspectos:

- A capacidade de atendimento às necessidades identificadas;
- O grau de maturidade tecnológica das soluções;
- A viabilidade de implantação no ambiente institucional;
- A compatibilidade com o modelo operacional do órgão;
- A possibilidade de contratação como serviço, com suporte e atualizações.

O levantamento foi realizado de forma segmentada para os Itens 1 (EDR) e 2 (SEG), considerando as especificidades técnicas de cada vetor de proteção e a necessidade de orquestração entre ambos.

8.1 Levantamento de Soluções – Item 1: Proteção de Endpoints (EDR)

Para o atendimento da necessidade de proteção de endpoints, foram identificadas e analisadas três alternativas estratégicas:

Solução 1 – Manutenção da tecnologia atualmente utilizada (Renovação)

Consiste na continuidade do licenciamento da solução de proteção de endpoint em uso, mantendo o modelo operacional vigente.

Análise Técnica: Esta alternativa apresenta obsolescência tecnológica diante do cenário de ataques *fileless* e de ransomware modernos. Por se basear predominantemente na proteção de endpoints individuais, a solução atual gera uma "lacuna de visibilidade" (*Detection Gap*), incapaz de identificar movimentos laterais e técnicas de persistência de invasores. Além disso, impõe um alto custo operacional à equipe técnica, devido à necessidade de intervenções manuais constantes para a análise de falsos positivos e a remediação local de ativos.

Solução 2 – Aquisição de Solução Tradicional de Endpoint Protection (EPP)

Consiste na substituição da solução atual por outra ferramenta de mercado com arquitetura semelhante.

Análise Técnica: Embora possa oferecer uma interface mais moderna, esta alternativa mantém uma postura reativa, carecendo de capacidades de investigação forense e resposta ativa. Em caso de uma infecção que contorne a barreira inicial, a TI permaneceria "cega" quanto à origem do incidente e enfrentaria dificuldades técnicas para realizar a contenção remota dos 1.905 ativos, mantendo o risco de paralisia institucional elevado.

Solução 3 – Aquisição de Solução com capacidades de Detecção e Resposta em Endpoint (EDR)

Consiste na migração para uma plataforma moderna de EDR - Endpoint Defense and Response, que integra prevenção (EPP) ao monitoramento comportamental contínuo e à resposta automatizada.

Análise Técnica: É a única alternativa que atende plenamente às Necessidades de Negócio do Inmetro. Esta solução permite a detecção de anomalias em tempo real por meio de Inteligência Artificial, proporcionando visibilidade total sobre a "linhagem" dos ataques. Suas capacidades de isolamento lógico de resposta remota centralizada reduzem drasticamente o tempo de resposta, permitindo que a equipe técnica gerencie incidentes de forma estratégica e automatizada, independentemente da localização física do ativo.

8.2 Levantamento de Soluções – Item 2: Proteção de Correio Eletrônico (SEG)

Para o atendimento da necessidade de proteção do correio eletrônico, foram identificadas e analisadas três alternativas estratégicas:

Solução 1 – Manutenção da tecnologia atualmente utilizada (Renovação)

Consiste na continuidade do licenciamento do gateway de e-mail em uso, mantendo a arquitetura operacional atual.

Análise Técnica: Esta alternativa é tecnicamente inviável devido à sua obsolescência funcional. A solução atual não permite atualização para versões suportadas pelo fabricante, o que a torna vulnerável a explorações conhecidas. Além disso, apresenta baixa eficácia contra ataques modernos de Engenharia Social (BEC e Spear Phishing), gerando um alto volume de incidentes que demandam intervenção manual da TI e expondo os servidores legados (Exchange 2010 e Zimbra) a riscos de comprometimento sistêmico.

Solução 2 – Aquisição de Solução de Filtragem Básica

Consiste na substituição da solução atual por ferramentas de filtragem de e-mail convencionais, focadas na reputação de IP e em assinaturas de spam conhecidas.

Análise Técnica: Esta alternativa oferece proteção superficial, insuficiente para o perfil de ameaças direcionadas a órgãos da Administração Pública Federal. Soluções básicas carecem de recursos de análise dinâmica de URLs (Time-of-Click) e de inspeção de anexos no Sandbox, o que permite a passagem de links maliciosos que são ativados após a entrega. Adicionalmente, costumam apresentar limitações severas de integração com diretórios LDAP/Linux, o que dificulta a governança de acesso e a segregação de funções exigidas pelo Inmetro.

Solução 3 – Aquisição de Solução Avançada de Secure Email Gateway (SEG)

Consiste na adoção de uma plataforma moderna de gateway de e-mail, com inteligência artificial e capacidades de inspeção profunda do conteúdo.

Análise Técnica: É a única alternativa que oferece a "Blindagem Ativa" necessária para o ambiente heterogêneo do Inmetro. Esta solução integra mecanismos de Sandbox nativos, detecção de fraudes de personificação (BEC - Business E-mail Compromise) e inspeção de vetores modernos como QR Codes. Sua arquitetura permite a plena compatibilidade com ambientes Linux/Zimbra e integração nativa ao diretório LDAP, garantindo que a segurança do e-mail atue em conjunto com as demais camadas de defesa da Instituição.

8.3 Considerações Gerais sobre as Soluções Levantadas

As alternativas identificadas refletem diferentes estágios de maturidade tecnológica e modelos de proteção disponíveis no mercado global. A inclusão das alternativas de manutenção das soluções vigentes (Soluções 1) e de tecnologias convencionais (Soluções 2) visa estabelecer um referencial comparativo direto, permitindo avaliar o hiato de proteção existente entre as ferramentas atuais e as necessidades de resiliência cibernética do Inmetro diante das ameaças modernas.

É importante ressaltar que, embora as soluções tradicionais ou básicas possam apresentar menor complexidade imediata de aquisição, demonstram insuficiência técnica para mitigar riscos críticos, como ransomware de dia zero e fraudes de personificação, além de não proverem o nível de automação necessário para uma equipe técnica enxuta.

Por outro lado, as soluções modernas e avançadas (Soluções 3) alinham-se aos objetivos estratégicos da Instituição, proporcionando a inteligência, a visibilidade e a interoperabilidade necessárias para a proteção de ambientes heterogêneos e legados (Exchange/Zimbra).

Desta forma, o levantamento realizado não se restringe à funcionalidade básica, mas considera o ciclo de vida das tecnologias e a eficácia na mitigação proativa de riscos. No item seguinte, procede-se à análise comparativa e à seleção da alternativa que apresenta o melhor equilíbrio entre eficácia técnica e viabilidade econômica para o atendimento definitivo da demanda.

9. Análise comparativa de soluções

A análise comparativa das alternativas levantadas considera aspectos qualitativos e técnicos, avaliando o grau de aderência às necessidades de negócio e tecnológicas identificadas neste Estudo Técnico Preliminar, bem como os riscos e benefícios associados a cada cenário.

9.1 Análise Comparativa – Item 1: Proteção de Endpoints (EDR)

Considerações Iniciais: A alternativa de renovação da solução atual apresenta, em teoria, a vantagem da continuidade operacional imediata e a familiaridade da equipe com a interface de gestão. Contudo, essa vantagem é suplantada pelo elevado risco de segurança, uma vez que a ferramenta não acompanhou a evolução das ameaças. Manter a solução atual resultaria em um "falso senso de segurança", mantendo o Inmetro vulnerável a ataques que a tecnologia vigente não consegue detectar. As soluções tradicionais de mercado (EPP), por outro lado, oferecem apenas melhorias incrementais na interface, sem resolver a lacuna crítica de visibilidade e de resposta.

Quadro comparativo – Item 1

CrITÉrios e Requisitos Técnicos	Solução 1 (Renovação Atual)	Solução 2 (Proteção Tradicional - EPP)	Solução 3 (EDR Moderno)
Atendimento às necessidades de negócio	Insuficiente	Parcialmente	Pleno
Detecção Comportamental e IA (Zero-Day)	Não atende	Parcialmente	Pleno
Resposta e Contenção Remota (Isolamento)	Não atende	Não atende	Pleno
Automação de respostas	Não atende	Não atende	Pleno
Visibilidade de Ativos Fora da Rede	Limitada	Parcialmente	Pleno
Investigação Forense e Causa Raiz	Não atende	Não atende	Pleno
Recuperação de Ransomware (Rollback)	Não atende	Não atende	Pleno
Redução da Carga de Trabalho Manual	Não atende	Parcialmente	Pleno
Resultado da análise	Não viável	Não viável	Viável

Síntese da Análise – Item 1. A análise demonstra que as Soluções 1 e 2 não conferem a resiliência necessária ao cenário atual de ameaças cibernéticas. A renovação da solução atual (Solução 1) perpetuaria vulnerabilidades críticas, enquanto a adoção de uma proteção tradicional (Solução 2) falharia em proporcionar visibilidade e resposta ativa. A Solução de Detecção e Resposta em Endpoint (EDR) apresenta-se como a única alternativa tecnicamente viável, pois automatiza a detecção de ameaças complexas, permite a contenção remota de incidentes e otimiza o uso da capacidade da equipe técnica, garantindo a continuidade das operações do Inmetro com o nível de proteção exigido pela SGD/MGI e pelo GSI/PR.

9.2 Análise Comparativa – Item 2: Proteção de Correio Eletrônico (SEG)

Considerações Iniciais. A alternativa de renovação da solução atual apresenta a vantagem teórica de manter o status quo operacional. Contudo, essa permanência representa um risco estratégico inaceitável, visto que a ferramenta vigente atingiu o limite de sua vida útil (obsolescência), sendo incapaz de receber atualizações de segurança do fabricante. Em um ambiente com servidores legados (Exchange 2010 e Zimbra), o gateway de e-mail deve atuar como um escudo reforçado, portanto manter a solução atual é deixar a principal porta de entrada de ataques do Inmetro vulnerável a fraudes modernas (BEC e Phishing de QR Code) que a tecnologia atual sequer consegue processar. Da mesma forma, as soluções básicas de filtragem (Solução 2) oferecem apenas uma troca de fabricante sem salto tecnológico real, por carecerem de motores de análise dinâmica (Sandbox) e remediação pós-entrega, elas falham em prover a "blindagem" necessária para os servidores legados (Exchange 2010 e Zimbra), mantendo o Inmetro em um estado de proteção reativo e insuficiente.

Quadro comparativo – Item 2

Critérios e Requisitos Técnicos	Solução 1 (Renovação Atual)	Solução 2 (Filtragem Básica)	Solução 3 (SEG Avançado)
Atendimento às necessidades de negócio	Insuficiente	Insuficiente	Pleno
Detecção de BEC e Fraudes de Identidade	Não atende	Insuficiente	Pleno
Sandbox e Proteção de URL (Time-of-Click)	Não atende	Não atende	Pleno
Inspeção de QR Code e Vetores Modernos	Não atende	Não atende	Pleno
Compatibilidade Nativa Linux / LDAP	Não atende	Parcialmente	Pleno
Gestão Granular e Perfis (RBAC)	Não atende	Parcialmente	Pleno
Remediação Pós-Delivery (Exchange /Zimbra)	Não atende	Não atende	Pleno
Resultado da análise	Não viável	Não viável	Viável

Síntese da Análise – Item 2. A renovação da solução atual (Solução 1) é tecnicamente desaconselhável por perpetuar uma infraestrutura obsoleta e sem suporte a atualizações de segurança. Embora as soluções de mercado classificadas como tradicionais ou básicas (Soluções 2) possam atender, isoladamente, a alguns requisitos funcionais, elas falham em oferecer o conjunto integral e indissociável de capacidades exigido pelo ambiente institucional. A ausência de recursos críticos (como o Sandbox e o Isolamento Remoto no Item 1, ou a Inspeção de QR Code e a Remediação Pós-Delivery no Item 2) torna essas alternativas insuficientes para mitigar os riscos associados aos sistemas legados e às ameaças modernas, o que resulta em sua classificação como tecnicamente inviáveis para esta contratação. A Solução Avançada de Secure Email Gateway (SEG) é a única alternativa que

oferece a proteção proativa necessária, garantindo a interoperabilidade e assegurando a continuidade das comunicações oficiais do Inmetro, com o nível de governança exigido.

9.3 Conclusão da Análise Comparativa

Com base na análise realizada, conclui-se que:

- As alternativas de renovação das soluções atuais, embora apresentem vantagens operacionais pontuais, não atendem plenamente às necessidades institucionais;
- As soluções tradicionais ou básicas apresentam limitações relevantes;
- As soluções modernas e avançadas (EDR e SEG) são as únicas que atendem de forma satisfatória às necessidades de negócio e tecnológicas identificadas neste ETP.

9.4 Alternativas Escolhidas

Conforme as análises acima citadas, a solução escolhida para o item 1 foi a **Solução 3 – Aquisição de Solução com capacidades de Detecção e Resposta em Endpoint (EDR)**, por trazer mais benefícios para o Inmetro.

A solução escolhida para o item 2 foi a **Solução 3 – Aquisição de Solução Avançada de Secure Email Gateway (SEG)**, por trazer mais benefícios para o Inmetro.

REQUISITOS	ITEM 1 - SOLUÇÃO 3	ITEM 2 - SOLUÇÃO 3
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	Sim	Sim
A Solução está disponível do Portal do Software Público	Não	Não
A Solução é composta por software livre ou software público?	N/A	N/A
Aderente ao e-MAG?	N/A	N/A
Aderente ao e-Ping?	N/A	N/A
Aderente ao ePwg?	N/A	N/A
Aderente ao Icp-Brasil?	N/A	N/A
Aderente ao e-ARQ Brasil?	N/A	N/A
Atende ao padrão Design System de governo?	N/A	N/A
Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual?	Não	Não
Resultado da Análise	Viável	Viável

10. Registro de soluções consideradas inviáveis

Em conformidade com o § 1º do art. 11 da Instrução Normativa SGD/ME nº 94, de 2022, registram-se, a seguir, as soluções identificadas no levantamento e consideradas inviáveis para atendimento da demanda, dispensando-se o cálculo do Custo Total de Propriedade (TCO) dessas alternativas, em razão de sua inadequação técnica.

10.1 Item 1: Proteção de Endpoints (EDR)

Foram consideradas **inviáveis** as seguintes soluções:

Solução 1 - Manutenção (renovação) da solução atualmente utilizada, em razão de:

- Ausência de capacidades adequadas de detecção comportamental;
- Inexistência de funcionalidades de resposta a incidentes;
- Baixo nível de automação frente ao cenário atual de ameaças;

- Maior dependência de atuação manual da equipe técnica, o que não é compatível com a capacidade operacional existente.

Solução 2 - Aquisição de solução tradicional de EPP, por não contemplar de forma satisfatória funcionalidades essenciais de resposta, de correlação de eventos e de apoio à investigação de incidentes.

10.2 Item 2: Proteção de Correio Eletrônico (SEG)

Foram consideradas **inviáveis** as seguintes soluções:

Solução 1 - Manutenção (renovação) da solução atualmente utilizada, em razão de:

- Baixa eficácia na detecção de mensagens de phishing;
- Limitações administrativas e operacionais relevantes;
- Incompatibilidade tecnológica com o ambiente institucional;
- Impossibilidade de evolução e de atualização da solução.

Solução 2 - Aquisição de solução básica de filtragem de e-mails, por apresentar recursos limitados diante das necessidades atuais de detecção de ataques de engenharia social, análise de links e anexos e automação de respostas.

As soluções acima não atendem adequadamente às necessidades de negócio e tecnológicas identificadas, razão pela qual foram descartadas.

11. Análise comparativa de custos (TCO)

A estimativa preliminar registrada no Documento de Formalização da Demanda (DFD) foi de R\$ 1.099.759,49 (um milhão, noventa e nove mil, setecentos e cinquenta e nove reais e quarenta e nove centavos), calculada com base nos valores históricos dos contratos vigentes, atualizados pelo Índice de Custos de Tecnologia da Informação (ICTI) acumulado de 11,1790% (período base ref. setembro/2025). Ressalta-se que o valor final de referência para a licitação será obtido por meio de ampla Pesquisa de Preços de Mercado, a ser consolidada na fase de elaboração do Termo de Referência, visando refletir o custo real de mercado de soluções dotadas de tecnologias Next-Gen (EDR e SEG) e de capacidades de automação.

Em conformidade com a IN SGD/ME nº 94/2022, procedeu-se à análise do Custo Total de Propriedade (Total Cost of Ownership – TCO) das soluções consideradas tecnicamente viáveis ao longo de um ciclo de 36 (trinta e seis) meses. A análise concentrou-se nos custos diretos de subscrição e implantação, adotando-se as seguintes premissas para os custos indiretos:

11.1 Justificativa de Neutralidade de Custos de Infraestrutura.

Em relação aos custos indiretos (energia elétrica, refrigeração e espaço físico), optou-se pela não valoração monetária específica nestes itens, fundamentada nas seguintes razões:

Neutralidade de Recursos: A Solução de Proteção de Correio Eletrônico (SEG) será instalada na infraestrutura de virtualização já existente, substituindo a solução legada. Assim, haverá uma substituição direta de recursos computacionais, sem gerar demanda incremental significativa de energia ou climatização no Data Center;

Desoneração de Infraestrutura: A solução de proteção de endpoint (EDR) será implementada preferencialmente no modelo de nuvem, desonerando o ambiente local de processamento e de armazenamento de logs, o que, em tese, reduz indiretamente a ocupação de recursos do Data Center institucional.

Limitação de Medição Granular: O órgão não dispõe de ferramentas para a medição isolada do consumo de energia por ativo de TI, o que tornaria qualquer valoração deste item meramente estimativa e passível de imprecisões.

11.2 Eficiência Operacional e Custo do Risco.

Embora as Soluções Avançadas (Soluções 3) possam apresentar um custo de subscrição superior às ferramentas tradicionais, a análise de TCO deve considerar a redução drástica do esforço manual da equipe técnica. A automação das respostas a incidentes e a redução de falsos positivos otimizam a capacidade produtiva do Inmetro. Adicionalmente, deve-se considerar o Custo do Risco Institucional: o investimento em tecnologias de detecção e resposta (EDR/Sandboxing) justifica-se pela mitigação do risco de incidentes de *ransomware*, cujos custos de recuperação de dados, paralisação de serviços e danos à imagem institucional seriam de ordem de grandeza superior ao valor desta contratação.

Por fim, a análise de custos foi realizada apenas para as soluções consideradas viáveis, conforme estabelecido na IN SGD/ME nº 94, de 2022.

11.3 Cálculo do Custo Total de Propriedade (TCO)

O cálculo do TCO para as soluções consideradas tecnicamente viáveis (Soluções 3) reflete o investimento necessário para a cobertura integral do ambiente durante o ciclo de vida do contrato.

Foi elaborada a Nota Técnica nº 41/2026/Diinf/Ctinf-Inmetro de Análise fundamentada da pesquisa de preços onde foram determinados os valores estimados da contratação conforme abaixo.

Solução Viável – Item 1 - Proteção de Endpoints (EDR)

Componentes de custo considerados:

- Subscrição de licenciamento pelo período de 36 meses;
- Suporte técnico 24x7 e direito à atualização tecnológica;
- Serviços profissionais de instalação, configuração, tuning e operação assistida.

Ano	Custo estimado (R\$)
Ano 1	398.449,80
Ano 2	0,00
Ano 3	0,00
TCO – 36 meses	398.449,80

* Nota explicativa: Conforme a estratégia de contratação definida, o modelo prevê pagamento único após a aceitação definitiva da solução. Para fins de empenho e reserva orçamentária, o valor total da subscrição de 36 meses é alocado integralmente no primeiro exercício, garantindo a disponibilidade dos recursos necessários à vigência plurianual do licenciamento e dos serviços associados.

Solução Viável – Item 2: Proteção de Correio Eletrônico (SEG)

Componentes de custo considerados:

- Subscrição de licenciamento pelo período de 36 meses;
- Suporte técnico 24x7 e direito à atualização tecnológica;
- Serviços profissionais de instalação, configuração, tuning e operação assistida.

Ano	Custo estimado (R\$)
Ano 1	1.083.134,25
Ano 2	0,00
Ano 3	0,00
TCO – 36 meses	1.083.134,25

* Nota explicativa: Conforme a estratégia de contratação definida, o modelo prevê pagamento único após a aceitação definitiva da solução. Para fins de empenho e reserva orçamentária, o valor total da subscrição de 36 meses é alocado integralmente no primeiro exercício, garantindo a disponibilidade dos recursos necessários à vigência plurianual do licenciamento e dos serviços associados.

11.4 Mapa Comparativo dos Custos Totais de Propriedade (TCO)

Solução	TCO estimado – 36 meses
Solução EDR (Item 1)	R\$ 398.449,80
Solução Avançada de E-mail Gateway (Item 2)	R\$ 1.083.134,25

12. Descrição da solução de TIC a ser contratada

Com base na análise de alternativas e no levantamento das necessidades institucionais realizado neste Estudo Técnico Preliminar, a solução de TIC a ser contratada consiste em um Ecossistema de Segurança de Nova Geração, composto por duas plataformas integradas e complementares, conforme detalhado abaixo:

12.1 Item 1: Proteção de Endpoints (EDR)

A solução consiste em uma plataforma de Detecção e Resposta em Endpoints (EDR) para proteção de 1.905 ativos (estações de trabalho e servidores) em ambiente multiplataforma (Windows, Linux e MacOS).

- Escopo: Substituição do modelo preventivo tradicional por uma tecnologia baseada em inteligência comportamental e análise de eventos em tempo real;
- Modelo de Entrega: Subscrição por 36 meses, com gerenciamento centralizado (preferencialmente em nuvem), garantindo visibilidade de ativos dentro e fora da rede institucional;
- Capacidades Centrais: Detecção proativa (IA), isolamento lógico de máquinas, resposta remota e recuperação automatizada de ataques (*Rollback*).

12.2 Item 2: Proteção de Correio Eletrônico (SEG)

A solução consiste em um Gateway de Segurança de E-mail (Secure Email Gateway – SEG) para proteção de 2.675 contas, atuando como uma blindagem ativa para os servidores de correio eletrônico institucional.

- Escopo: Proteção avançada do fluxo de mensagens (inbound/outbound) contra ataques de Business Email Compromise (BEC), Phishing (incluindo QR Code) e Malware;
- Modelo de Entrega: Subscrição por 36 meses, com implantação on-premise (local), garantindo a interoperabilidade com sistemas legados (Exchange 2010 e Zimbra) e diretórios corporativos (LDAP/Linux);
- Capacidades Centrais: Análise dinâmica em Sandbox com proteção contra e-mails contendo URLs e arquivos maliciosos.

12.3 Serviços e Suporte Associados (Comuns aos Itens 1 e 2)

A contratação inclui, de forma indissociável das subscrições:

- Serviços Profissionais: Instalação técnica, configuração de políticas de segurança, processo de tuning (calibragem) e operação assistida durante a fase inicial;
- Transferência de Conhecimento: Treinamento operacional (hands-on) para a equipe técnica do Inmetro;
- Suporte e Manutenção: Atendimento técnico especializado em regime 24x7, com direito à atualização tecnológica contínua durante todo o período de vigência.

As características técnicas granulares e os critérios mandatórios de aceitação de cada item estão detalhados no ANEXO I (EDR) e no ANEXO II (SEG) deste Estudo Técnico Preliminar.

Aquisição de Solução de Segurança da Informação (TIC), incluindo licenciamento por subscrição, serviços de instalação, configuração, operação assistida, treinamento, suporte e manutenção, voltadas à Proteção de Endpoints (EDR - Endpoint Detect and Response) e Proteção de Correio Eletrônico (SEG - Secure E-mail Gateway), pelo prazo de 36 (trinta e seis) meses.

ITEM	DESCRIÇÃO	CATSER	UNIDADE	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01	Proteção de Endpoints (EDR - Endpoint Detect and Response)	27502	unidade	1.905	R\$ 209,16	R\$ 398.449,80
02	Proteção de Correio Eletrônico (SEG - Secure E-mail Gateway)	27502	unidade	2.675	R\$ 404,91	R\$ 1.083.134,25

13. Estimativa de custo total da contratação

Valor (R\$): 1.481.584,05

O valor estimado da contratação é de R\$ 1.481.584,05 (um milhão, quatrocentos e oitenta e um mil, quinhentos e oitenta e quatro reais e cinco centavos), com prazo de vigência de 12 (doze) meses, contados da assinatura do contrato, na forma do artigo 105 da Lei nº 14.133/2021.

ITEM	DESCRIÇÃO	CATSER	UNIDADE	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
01	Proteção de Endpoints (EDR - Endpoint Detect and Response)	27502	unidade	1.905	R\$ 209,16	R\$ 398.449,80
02	Proteção de Correio Eletrônico (SEG - Secure E-mail Gateway)	27502	unidade	2.675	R\$ 404,91	R\$ 1.083.134,25

14. Justificativa técnica da escolha da solução

A escolha pelas soluções descritas neste Estudo Técnico Preliminar (ETP) decorre da análise técnica, operacional e econômica de alternativas, considerando a necessidade premente de modernização da defesa cibernética do Inmetro. A decisão prioriza a resiliência institucional e a continuidade dos serviços públicos diante de um cenário de ameaças que as ferramentas atuais já não são capazes de mitigar.

14.1 Item 1: Proteção de Endpoints (EDR)

A análise técnica demonstrou que a transição para uma solução de EDR é a única via para sanar a "lacuna de detecção" do modelo preventivo tradicional. Embora a renovação da solução atual apresente a vantagem da familiaridade operacional, tal benefício é suplantado pelo elevado risco de segurança, visto que a ferramenta vigente carece de inteligência comportamental para conter ataques *fileless* e ransomware de dia zero. A escolha pelo EDR justifica-se pela capacidade de isolamento remoto e de investigação forense, permitindo que a equipe técnica responda a incidentes em tempo real, sem a necessidade de intervenções físicas, otimizando a força de trabalho e elevando o nível de proteção de 1.905 ativos institucionais.

14.2 Item 2: Proteção de Correio Eletrônico (SEG)

No que se refere à proteção do correio eletrônico, a escolha por uma solução avançada de gateway (SEG) justifica-se pela obsolescência funcional e tecnológica da ferramenta atual, que se mostra ineficaz contra ataques de Engenharia Social (BEC e Phishing de QR Code). Em um ambiente que mantém servidores legados (Microsoft Exchange 2010 e Zimbra 8.x), a adoção de uma solução com Sandbox e proteção Time-of-Click se mostra obrigatória para atuar como blindagem ativa, protegendo serviços que não recebem mais atualizações de segurança.

14.3 Avaliação integrada e decisão

A análise integrada demonstra que a substituição das soluções vigentes por tecnologias de Nova Geração (EDR e SEG) é a alternativa que melhor atende ao interesse público. Os ganhos em automação, visibilidade e eficácia defensiva superam amplamente a conveniência de manter o conhecimento das ferramentas atuais. A decisão pela Solução 3 para ambos os itens garante a defesa em profundidade, na qual o monitoramento do endpoint e a filtragem do e-mail operam de forma orquestrada. Essa escolha está devidamente alinhada às boas práticas de segurança da informação, às diretrizes de governança da Secretaria de Governo Digital (SGD/MGI) e às normas do Gabinete de Segurança Institucional (GSI/PR), assegurando a integridade dos dados institucionais do Inmetro e a continuidade das comunicações oficiais pelos próximos 36 meses.

15. Justificativa econômica da escolha da solução

Considerando as características distintas dos objetos a serem contratados, optou-se pelo parcelamento da contratação por itens, em detrimento da contratação em lote único. Sob o aspecto técnico, as soluções de proteção de endpoints e de correio eletrônico possuem finalidades, arquiteturas, modelos de licenciamento e requisitos operacionais distintos, o que justifica sua contratação de forma independente, permitindo maior aderência às necessidades específicas de cada solução.

Sob o aspecto econômico e concorrencial, o parcelamento por itens amplia a competitividade do certame, possibilitando a participação de um maior número de fornecedores, inclusive empresas que não possuem capacidade de fornecer soluções distintas de forma conjunta. Essa estratégia contribui para a obtenção de melhores condições de preço e qualidade para a Administração Pública, além de reduzir o risco de concentração de mercado em um único fornecedor.

Adicionalmente, a contratação por itens facilita a gestão e a fiscalização contratual, reduz riscos operacionais e permite maior controle sobre a execução dos serviços, especialmente considerando que se trata de soluções estratégicas para a segurança da informação institucional. Dessa forma, o parcelamento da contratação por itens mostra-se tecnicamente e economicamente mais vantajoso para a Administração.

16. Benefícios a serem alcançados com a contratação

A contratação das soluções de proteção de endpoints e de correio eletrônico proporcionará benefícios relevantes à Administração, contribuindo diretamente para o fortalecimento da segurança da informação e para a continuidade dos serviços institucionais.

Entre os principais benefícios esperados, destacam-se:

- Redução do risco de incidentes de segurança da informação, especialmente aqueles originados em endpoints e no correio eletrônico, principais vetores de ataques cibernéticos atualmente;
- Aumento da capacidade de prevenção, detecção e resposta a ameaças, por meio da adoção de soluções mais modernas, automatizadas e alinhadas ao estado da arte em segurança cibernética;
- Maior continuidade e disponibilidade dos serviços institucionais, minimizando o risco de interrupções causadas por ataques cibernéticos, como ransomware, phishing e comprometimento de contas;
- Fortalecimento da governança de segurança da informação, com maior visibilidade sobre eventos, incidentes e tendências de ameaças, apoiando a tomada de decisão e o acompanhamento gerencial;
- Redução do impacto operacional de incidentes de segurança, diminuindo o tempo de resposta e recuperação, bem como os esforços necessários para contenção e mitigação de ataques;
- Otimização do uso dos recursos humanos da área de Tecnologia da Informação, com redução de atividades manuais e repetitivas, permitindo que a equipe técnica concentre seus esforços em atividades estratégicas e de maior valor agregado;
- Modernização das soluções de segurança institucional, substituindo ferramentas que não acompanham a evolução das ameaças e das tecnologias utilizadas no ambiente corporativo;
- Aumento do nível de proteção aos usuários finais, reduzindo a exposição a mensagens fraudulentas, códigos maliciosos e tentativas de fraude, o que contribui para um ambiente digital mais seguro.

17. Providências a serem Adotadas

Aprovação da entidade máxima de TIC;

Aprovação da Alta Administração do Inmetro;

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

O presente planejamento foi elaborado em conformidade com a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, bem como com a Instrução Normativa nº 40, de 22 de maio de 2020, observando os requisitos técnicos, administrativos e estratégicos aplicáveis à contratação de soluções de Tecnologia da Informação.

A análise realizada demonstra que a contratação proposta atende adequadamente às necessidades de negócio, aos requisitos técnicos e operacionais e aos objetivos estratégicos do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro, especialmente no que se refere ao fortalecimento da segurança da informação e à continuidade dos serviços institucionais.

As soluções avaliadas mostram-se tecnicamente viáveis, compatíveis com o ambiente tecnológico existente e alinhadas às boas práticas de segurança cibernética, oferecendo maior capacidade de prevenção, detecção e resposta a incidentes, com níveis adequados de automação e governança.

Sob o aspecto técnico-econômico, a solução proposta apresenta-se como a alternativa mais vantajosa para a Administração Pública Federal, considerando a relação custo-benefício, a redução de riscos operacionais, a mitigação de impactos decorrentes de incidentes de segurança e a otimização do uso dos recursos humanos disponíveis.

O presente Estudo Técnico Preliminar tem por objetivo a contratação de soluções de segurança da informação, incluindo licenciamento por subscrição, suporte, atualizações e serviços associados, voltadas à proteção de endpoints e do correio eletrônico institucional, não se tratando de aquisição de equipamentos de infraestrutura ou de ativos de data center.

Por fim, a contratação proposta contribui para a modernização das soluções de segurança institucional, elevando o nível de proteção do ambiente de Tecnologia da Informação do Inmetro e assegurando maior resiliência cibernética, em alinhamento com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e com os objetivos institucionais do órgão.

Com base nas informações levantadas ao longo deste Estudo Técnico Preliminar, a Equipe de Planejamento da Contratação declara que a contratação é VIÁVEL e, do ponto de vista técnico e econômico, essencial para o atendimento às necessidades do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro.

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: Portaria Inmetro/DIRAF nº 7, de 29 de janeiro de 2026

PAULO GUSTAVO DE OLIVEIRA DEL PELOSO

Integrante Requisitante



Assinou eletronicamente em 25/05/2026 às 11:04:02.

Despacho: Portaria Inmetro/DIRAF nº 7, de 29 de janeiro de 2026

ANDRE GHEVENTER

Integrante Técnico



Assinou eletronicamente em 25/05/2026 às 11:29:57.

Despacho: Portaria Inmetro/DIRAF nº 7, de 29 de janeiro de 2026

LUIZ FERNANDO FERREIRA DE MEDEIROS LIMA

Integrante Técnico



Assinou eletronicamente em 25/05/2026 às 11:23:25.