INFRA S.A.

Estudo Técnico Preliminar da Contratação/GEINF-INFRASA/SUPTI-INFRASA/DIMEI-INFRASA/DIREX-INFRASA/CONSAD-INFRASA/AG-INFRASA-INFRASA

Brasília, 11 de dezembro de 2024.

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO DE TIC

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. A segurança da informação vem evoluindo e crescendo continuamente nas últimas décadas e, no mundo digital e interconectado, se denomina cibersegurança ou segurança cibernética, caracterizada pelo gerenciamento de riscos de segurança da informação e a salvaguarda de pessoas, organizações e sociedades contra vulnerabilidades, ameaças e ataques, quando a informação está em forma digital em computadores, armazenamento e redes. Engloba também temas como continuidade de negócios e resiliência organizacional, tratamento e resposta a incidentes de segurança, forense digital.

1.2. O universo de cibersegurança é muito amplo e complexo. Exige conhecimentos altamente especializados, atualização constante, atuação dinâmica e eficaz, em suma, grandes e variados esforços, organização, orquestração e governança em termos de processos, pessoas e ferramentas. Organizações de referência internacional, governamentais e independentes da comunidade, tem difundido e atualizado constantemente inúmeros padrões, modelos (frameworks) e melhores práticas de cibersegurança: International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) dos Estados Unidos, Center for Internet Security (CIS), MITRE (originário do Massachussets Institute of Technology), a fundação de código aberto Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), dentre outras.

1.3. Recentemente, diversos fatores ampliaram e aceleraram os desafios e necessidades de forma urgente:

- O uso ainda mais crítico, intensivo, complexo e distribuído de tecnologia da informação, serviços e recursos digitais nas atividades fim e administrativas, dentro e fora das dependências da empresa, com a implantação do teletrabalho e da crescente adoção de serviços em nuvem;
- As demandas decorrentes da entrada em vigor da Lei Federal nº 13.709 de 14/08/2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
- As exigências decorrentes da necessidade de estabelecer uma estratégia de segurança cibernética;
- Casos recentes cada vez mais frequentes de ameaças avançadas e direcionadas, incidentes em instituições públicas e privadas próximas, de ataques como ransomware (sequestro digital), fraudes, vazamento de dados, hacktivismo (ativismo político hacker).

1.4. Atualmente, há grande dificuldade em formar e contratar pessoal qualificado em segurança cibernética, pois a demanda está muito aquecida. Na Infra S.A., há ainda a dificuldade em viabilizar, do ponto de vista normativo e operacional, o uso de empregados públicos da estatal em regime de escalas de trabalho 24×7 para serviços contínuos e ininterruptos.

1.5. As tecnologias em cibersegurança têm avançado continuamente, incluindo a aplicação intensiva de inteligência artificial, aprendizado de máquina e automação, visando aumentar a eficiência e eficácia na detecção e resposta a ameaças e ataques, compensando parte da necessidade de atuação

humana.

1.6. Para evoluir seus recursos e enfrentar as atuais obrigações e ameaças cibernéticas, a Infra S.A. precisa realizar investimentos na tríade de pessoas, processos e tecnologias em governança, gestão e operações de segurança cibernética da empresa. O caminho natural para cumprir essa necessidade de forma ágil e adequada é recorrer ao mercado especializado, onde já existem provedores de serviços capazes de prover e operacionalizar o estado da arte em tecnologias e processos para cibersegurança, atuando com equipes de profissionais especializados e experientes.

1.7. Com o advento de novas ameaças tecnológicas, a Infra S.A. requer a adoção de novos mecanismos para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação. Os softwares e hardwares a serem implementados adicionarão camadas de segurança que abrangem desde a segurança do data center, o acesso remoto seguro, o processamento de dados e até backup.

1.8. Com a solução, será possível controlar todo o tráfego de dados e comunicação do ambiente interno com o externo, mitigando os riscos e ameaças cibernéticas, e estando apto a propiciar pronta resposta a eventuais incidentes ocorridos. Além disso, permitirá manter o controle das políticas de acesso à internet de acordo com o perfil dos contratados e terceirizados, garantindo a segurança no acesso à internet conforme os padrões estabelecidos pela organização.

1.9. A contratação proporcionará maior aderência aos padrões de mercado e adequação às legislações vigentes, como a LGPD e o Marco Civil da Internet, uma vez que a proteção para ativos de data center, rede e softwares é fundamental para o cumprimento da LGPD. Isso inclui funcionalidades que evitam acessos não autorizados na rede, vazamentos e roubos de informações, utilizando diversas tecnologias para proteção de rede. O acesso remoto seguro permitirá maior controle, diminuindo exponencialmente o risco de comprometimento da infraestrutura tecnológica.

1.10. A aquisição da pretensa solução é essencial para assegurar os requisitos de confidencialidade, disponibilidade e integridade das informações custodiadas pela Infra S.A., indispensáveis à continuidade do negócio e para o cumprimento de seus objetivos estratégicos.

1.11. Espera-se obter os seguintes resultados com a presente contratação:

1.11.1. Realizar ágil e investimentos na tríade de pessoas, processos e tecnologias em governança, gestão e operações de segurança cibernética da empresa, com aporte de pessoal técnico especializado, transferência de conhecimento, metodologia, padronização, estrutura operacional, ferramentas e soluções tecnológicas adequadas;

1.11.2. Prover meios adequados e especializados, em termos de pessoas, processos e tecnologias, para a gestão, implementação e manutenção eficaz dos controles e salvaguardas de segurança cibernética e prover o apoio à gestão e à governança da segurança da informação, à continuidade de negócios em TIC e à gestão de riscos na Infra S.A.;

1.11.3. Implantar um centro de controle e operações de segurança cibernética que componha as funções básicas de segurança de identificar, proteger, detectar, responder e recuperar, atuando tanto na segurança defensiva e reativa para monitoramento, detecção e resposta gerenciados a eventos e incidentes de segurança, quanto na segurança ofensiva e proativa para gestão contínua de vulnerabilidades e ameaças e para testes de segurança, prestando apoio direto às diversas áreas da Infra S.A. na prevenção, investigação, remediação e melhorias de cibersegurança;

1.11.4. Elevar o nível de segurança cibernética na Infra S.A., sua maturidade e melhoria contínua, visando estabelecer o nível adequado de controle sobre a confidencialidade, integridade e disponibilidade dos ativos e serviços de TIC e das informações digitais da estatal

1.11.5. Garantir conformidade e alinhamento com os requisitos de negócio, regulamentos pertinentes, a tolerância a riscos e os recursos da organização, em especial observância à estratégia de segurança cibernética da administração pública;

1.11.6. Obter visibilidade ampla sobre a segurança cibernética, a superfície de ataque e os níveis de risco na Infra S.A., tanto ao nível tático-operacional quanto ao nível estratégico-gerencial;

1.11.7. Contribuir na comunicação, difusão e disseminação da cultura e sensibilização dos conceitos, práticas e controles de segurança cibernética na Infra S.A.

1.12. **Necessidade da contratação:**

1.12.1. Com o advento de novas ameaças tecnológicas, a Infra S.A. requer a adoção de novos mecanismos para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação. Os softwares e hardwares a serem implementados adicionarão camadas de segurança que abrangem desde a segurança do data center, o acesso remoto seguro, o processamento de dados e até backup.

1.12.2. A contratação de um produto de simulação de ataques cibernéticos é essencial para:

a) **Identificar Vulnerabilidades:** Realizar testes contínuos e automatizados para identificar vulnerabilidades em sistemas, redes e aplicações antes que possam ser exploradas por agentes maliciosos;

b) **Avaliar a Eficácia das Defesas:** Simular ataques reais para avaliar a eficácia das defesas cibernéticas existentes e identificar áreas que necessitam de melhorias;

c) **Treinar Equipes de Segurança:** Proporcionar um ambiente seguro para que as equipes de segurança possam treinar e aprimorar suas habilidades na detecção e resposta a incidentes cibernéticos;

d) **Aprimorar a Resiliência Organizacional:** Aumentar a resiliência da organização contra-ataques cibernéticos, garantindo a continuidade dos negócios e a proteção dos dados;

e) **Cumprir Regulamentações:** Assegurar conformidade com regulamentações de segurança cibernética e privacidade de dados, como a LGPD, minimizando riscos legais e fortalecendo a confiança dos cidadãos.

1.12.3. Com a solução de simulação de ataques cibernéticos, será possível controlar todo o tráfego de dados e comunicação do ambiente interno com o externo, mitigando os riscos e ameaças cibernéticas, e estando apto a propiciar pronta resposta a eventuais incidentes ocorridos. Além disso, permitirá manter o controle das políticas de acesso à internet de acordo com o perfil dos contratados e terceirizados, garantindo a segurança no acesso à internet conforme os padrões estabelecidos pela organização.

1.12.4. A contratação proporcionará maior aderência aos padrões de mercado e adequação às legislações vigentes, como a LGPD e o Marco Civil da Internet, uma vez que a proteção para ativos de data center, rede e softwares é fundamental para o cumprimento da LGPD. Isso inclui funcionalidades que evitam acessos não autorizados na rede, vazamentos e roubos de informações, utilizando diversas tecnologias para proteção de rede. O acesso remoto seguro permitirá maior controle, diminuindo exponencialmente o risco de comprometimento da infraestrutura tecnológica.

1.12.5. A aquisição da pretensa solução é essencial para assegurar os requisitos de confidencialidade, disponibilidade e integridade das informações custodiadas pela Infra S.A., indispensáveis à continuidade do negócio e para o cumprimento de seus objetivos estratégicos.

1.13. **Problema a ser resolvido:**

1.13.1. A falta de mecanismos de segurança atualizados torna a Infra S.A. suscetível a acessos não autorizados e vazamentos de dados, dificultando o cumprimento das legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet. Portanto, a necessidade de adquirir novas soluções de tecnologia é essencial não apenas para a continuidade dos serviços, mas também para garantir a segurança da informação, eficiência operacional e a adequação às normas de segurança e proteção de dados.

1.13.2. A solução deve prover serviços gerenciados de segurança cibernética em três pilares:

- Governança e gestão de segurança cibernética de forma centralizada no âmbito de tecnologia da informação e comunicação (TIC), por meio de serviços estratégicos de governança, risco e conformidade (GRC) e definições de controles, salvaguardas e remediações;

- Segurança defensiva (*blue team*) por meio de monitoramento, detecção e resposta gerenciados de segurança cibernética;
- Segurança ofensiva (*red team*) por meio da gestão contínua de exposição a ameaças e vulnerabilidades, incluindo testes de segurança.

1.13.3. Além disso, aspectos urgentes e correlatos de gestão de identidade e acesso devem também ser avaliados, visando tanto entender e integrar adequadamente o cenário atual destes aspectos nos serviços abrangidos, quanto nortear as iniciativas futuras do Tribunal:

- Levantamento e diagnóstico inicial de governança e gestão de identidades (IGA), gestão de acessos e autorizações (AM) e segurança de aplicações de negócios (BAS).

1.13.4. A solução deve proporcionar simulação, avaliação e gestão estendida da postura de segurança da organização, permitindo medir a efetividade através de testes e avaliações do nível de proteção do perímetro e de ambientes internos para que haja uma compreensão completa quanto a efetividade dos controles de segurança.

1.13.5. A solução deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.

1.13.6. A plataforma deve fornecer minimamente um caminho para validação de brechas e simulações de ataques (BAS)

1.13.7. A solução deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.

1.13.8. A solução deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:

1.13.8.1. Reconhecimento – Validação de domínios e subdomínios a fim de identificar fraquezas e vulnerabilidades expostas na internet referente a organização. Nesta fase, a solução deverá utilizar de fontes de inteligência aberta (OSINT) para descoberta de credencias e outras informações as quais possam beneficiar um atacante.

1.13.8.2. Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalação de privilégio.

1.13.8.3. Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

1.13.8.4. Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais.

1.13.8.5. Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

1.13.9. A solução deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

1.13.10. A solução deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

1.13.11. A solução deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

1.13.12. As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

1.13.13. A solução deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

1.13.14. A solução deve possuir suporte e licenciamento realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

1.13.15. A solução deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

2. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO PARA A ESCOLHA DA SOLUÇÃO

2.1. A licitação terá por fundamento legal o regramento disposto na Lei nº 13.303/2016.

2.2. **Regem a presente demanda as seguintes legislações:**

2.2.1. Lei nº 13.303, de 30 de junho de 2016;

2.2.2. Instrução Normativa SGD/ME nº 94, de 2022;

2.2.3. Decreto nº 8.945, de 27 de dezembro de 2016;

2.2.4. Decreto nº 9.507, de 21 de setembro de 2018;

2.2.5. Regulamento Interno de Licitações e Contratos RILC;

2.2.6. Norma Interna de Licitações e Contratações Diretas da INFRA S.A.;

2.2.7. Plano Diretor de Tecnologia da Informação – PDTIC 2023-2025;

2.2.8. Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação;

2.2.9. Guia Nacional de Contratações Sustentáveis da Advocacia-Geral da União, 4ª edição, revista, atualizada, ampliada , de agosto de 2021.

2.2.10. Política de Transações com Partes Relacionadas no âmbito da VALEC - Engenharia, Construções e Ferrovias S.A., de 11 de maio de 2022.

2.2.11. Código de Ética da Valec, de 25 de junho de 2020.

2.2.12. Resolução CGPAR nº 29, de 5 de abril de 2022 : que estabelece orientações às empresas estatais federais para a contratação de bens e serviços de tecnologia da informação.

2.2.13. Resolução Normativa - INFRASA nº 10/2023/DIREX-INFRASA/CONSADINFRASA/AG-INFRASA: que Institui a Norma de Gestão e Fiscalização de Contratos.

2.2.14. Regimento Interno da Infra S.A., de 17 de agosto de 2023;

2.2.15. Estatuto Social da Infra S.A., de 8 de outubro de 2022.

2.2.16. Resolução VALEC nº 8/2021/CONSAD-VALEC, de 7 de abril de 2021: define a política de segurança da informação no âmbito da VALEC.

2.3. Os serviços serão prestados por empresa especializada no ramo, devidamente regulamentada e autorizada pelas autoridades competentes, em conformidade com a legislação vigente e padrões de sustentabilidade exigidos nesse instrumento e no futuro termo de referência.

2.4. **Requisitos de negócio:**

2.4.1. A Infra S.A. conta com uma estrutura computacional que visa garantir o cumprimento de sua missão institucional e atender às necessidades de tecnologia da informação e comunicação das diversas unidades organizacionais, usuários corporativos e externos.

2.4.2. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição da solução mais adequada a tais objetivos organizacionais, conforme relação a

seguir:

> I - Atender às demandas registradas no PDTIC relacionadas à aquisição de melhoria do parque computacional; e
> II - Prover recursos computacionais necessários ao perfeito desenvolvimento das atividades laborais, em relação aos recursos de hardware e software que provenham apoio à execução de tarefas da Infra S.A. relacionadas ao alcance mediato ou indireto do interesse público.

2.4.3. A presente contratação orienta-se pelos seguintes requisitos de negócio:

2.4.4. *Controle de Tráfego e Segurança:*

2.4.4.1. Ser capaz de controlar todo o tráfego de dados e comunicação entre o ambiente interno e externo, mitigando riscos e ameaças cibernéticas.

2.4.4.2. Possibilitar pronta resposta a incidentes e manter o controle das políticas de acesso à internet conforme o perfil dos contratados e terceirizados, garantindo a segurança no acesso à internet de acordo com os padrões estabelecidos pela organização.

2.4.5. *Desempenho e Escalabilidade:*

2.4.5.1. Permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar posturas de segurança cibernética de ponta a ponta.

2.4.5.2. Fornecer caminho para validação de brechas e simulação de ataques (BAS) utilizando táticas, técnicas e procedimentos que os atacantes e grupos criminosos cibernéticos utilizam.

2.4.6. *Suporte Técnico e Garantia:*

2.4.6.1. Suporte técnico 24 horas por dia, 7 dias por semana.

2.4.6.2. Atualizações de software conforme lançamentos, novos recursos, evoluções tecnológicas e correções de bugs e vulnerabilidades pelo fabricante.

2.4.7. *Continuidade Operacional:*

2.4.7.1. Mesmo após o término da garantia, os recursos e funcionalidades deverão permanecer operacionais, permitindo configurações pelos administradores.

2.4.7.2. Para softwares com licenciamento por subscrição, a manutenção das funcionalidades deverão ser realizadas através da renovação anual dos itens de atualização, subscrição, manutenção e suporte técnico.

2.4.8. *Atendimento Institucional:*

2.4.8.1. Prover à Infra S.A. os bens de TI necessários para o atendimento institucional.

2.4.8.2. Prover recursos que garantam melhor rendimento, eficiência e segurança na realização das atividades institucionais.

2.4.8.3. Prover condições tecnológicas necessárias para prestar atendimento de qualidade aos usuários finais.

2.4.9. *Disponibilidade e Performance:*

2.4.9.1. Garantir a disponibilidade dos serviços de TI demandados pelos usuários da Infra S.A.

2.4.9.2. Recursos que assegurem a performance adequada para acesso aos dados, informações e sistemas.

2.4.10. *Segurança Cibernética:*

2.4.10.1. Prover mecanismos que elevem o nível de segurança cibernética e protejam os sistemas desenvolvidos e administrados pela Infra S.A.

2.4.10.2. Prever ameaças cibernéticas, como malware, ataques de rede, injeções de

SQL e ataques de cross-site scripting.

2.4.11. *Transferência de Conhecimento:*

2.4.11.1. Prover repasse de conhecimento da solução implantada para a equipe técnica da Infra S.A.

2.4.11.2. Garantir que as configurações existentes continuem operacionais ou sejam migradas integralmente para uma nova solução, se necessário.

2.4.12. *Impacto Mínimo na Disponibilidade*:

2.4.12.1. Assegurar que a implantação da solução cause o menor impacto possível na disponibilidade dos serviços mantidos pela Infra S.A.

2.4.13. Conformidade e Continuidade dos Negócios:

2.4.13.1. Prover maior conformidade com regulamentações de segurança e privacidade de dados.

2.4.13.2. Possibilitar a continuidade dos negócios, prevenindo interrupções operacionais causadas por incidentes de segurança.

2.4.14. *Redução de Custos e Riscos:*

2.4.14.1. Diminuir custos associados à gestão de incidentes de segurança e violações.

2.4.14.2. Evitar roubo de dados sensíveis e mitigar acesso não autorizado.

2.4.14.3. Proteger contra monitoramento e interceptação de tráfego em redes Wi-Fi não seguras.

2.4.14.4. Reduzir ameaças internas e garantir armazenamento seguro.

2.5. **Requisitos de capacitação:**

2.5.1. A empresa contratada deverá fornecer capacitação na Solução ofertada para a equipe da Infra S.A., composta por uma turma de até 6 (seis) alunos.

2.5.2. O treinamento deverá ser ministrado em português (BR).

2.5.3. A carga horária mínima será de 16 (horas) pela solução ofertada.

2.5.4. O treinamento poderá ser realizado on-line, por meio da plataforma específica do fabricante, ou presencialmente, em local oferecido pela contratada.

2.5.5. A empresa deverá possuir conhecimento reconhecido pelo fabricante da solução ofertada.

2.5.6. Deverá ser fornecido material para o treinamento em formato PDF ou on-line.

2.5.7. Toda a infraestrutura, custos de material (apostilas, manuais, etc.), despesas do instrutor, entre outros serão de responsabilidade da contratada.

2.5.8. Os cursos deverão ser realizados em horários e datas a serem acordadas entre a contratada e a contratante.

2.5.9. A contratada será responsável por fornecer instalações com infraestrutura adequada para sala de treinamento na localidade a ser concordada entre as partes.

2.5.10. A Infra S.A. se resguarda o direito de acompanhar e avaliar a capacitação através de pesquisa de satisfação. Caso a capacitação não atinja uma pontuação superior a 80% (oitenta por cento), está deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional à Infra S.A.

2.5.11. Em caso de atualização das soluções durante o período de garantia, que introduza novas funcionalidades, poderá ser solicitado pela contratante um novo repasse de conhecimento correspondente a atualização, sem custo adicional à Infra S.A.

2.5.12. Ao final da capacitação, os participantes deverão estar aptos a administrar as soluções ofertadas de maneira eficaz.

2.5.13. Deverá ser fornecido certificado de participação a cada membro da equipe da Contratada que participar do processo de repasse de conhecimento, contendo pelo menos : nome do participante, carga horária, conteúdo programático e identificação do instrutor.

2.6. **Requisitos legais:**

2.6.1. Conforme pormenorizado no tópico 2.2 deste Estudo Técnico Preliminar da Contratação.

2.7. **Requisitos de manutenção:**

2.7.1. Garantia de atualização contínua e automática da base de dados de inteligência e ameaças cibernéticas, incluindo fontes públicas, Deep Web e Dark Web.

2.7.2. Durante toda prestação dos serviços a solução deverá contar com serviço de suporte online e on-site, no horário comercial, no prazo de 24 (vinte e quatro) meses, com atendimento remoto e presencial conforme demanda, garantindo a disponibilidade operacional ininterrupta da solução.

2.7.3. Realização de manutenções preventivas para garantir a integridade e desempenho da solução em alinhamento com os objetivos estratégicos da Infra S.A.

2.7.4. A CONTRATADA deverá prover o serviço de suporte e manutenção da solução, durante o período de vigência do contrato de suporte técnico e operação assistida, e deverá atender as seguintes premissas:

a) Chamados ilimitados para o suporte on-line e on-site;

b) Deverá ser fornecida uma Central de Atendimento (sítio na Internet, e-mail e telefone 0800), sem custo adicional para a CONTRATANTE para consultas, aberturas de chamados técnicos e envio de arquivos para análise.

2.8. **Requisitos temporais:**

2.8.1. Para essa demanda, deverá ser observado, ainda, o seguinte prazo principal:

2.8.1.1. Reunião Inicial: A CONTRATADA será convocada para reunião inicial correspondente ao contrato, a ser marcada pela fiscalização em até 5 (cinco) dias úteis após a publicação da portaria da Equipe de Gestão e Fiscalização. A reunião inicial poderá ser on-line ou de forma presencial;

2.8.1.2. Prazo de Entrega, Instalação e Realização dos Serviços: As soluções elencadas deverão ser entregues conforme os prazos constantes na tabela abaixo, contados da data de recebimento da Ordem de Fornecimento, em remessa única.

2.8.1.3. Local de entrega e instalação da solução: Na Sede da Infra S.A., localizada no Setor de Autarquias Sul (SAUS), Quadra 1, Bloco "G", Lotes 3 e 5 - Asa Sul, Brasília - DF, Brasil, CEP 70.070- 010; Telefones (61) 20296181 ou 2029-6134, em horário comercial, das 08h00 às 12h00 e das 14h00 às 17h00, de segunda-feira a sexta-feira, no 1º Subsolo, aos cuidados do Gerente de Infraestrutura e Tecnologia da Informação da Superintendência de Tecnologia da Informação - SUPTI. O endereço acima poderá ser alterado a qualquer momento mediante aviso prévio à CONTRATADA.

Descrição da Solução	**Prazos**	
	Entrega	**Instalação**
Contratação de aquisição de uma solução		30 dias corridos da data

abrangente para segurança cibernética(BAS), incluindo serviços gerenciados de segurança (MSS), simulação de violações e ataques cibernéticos, e ferramentas de monitoramento e resposta a incidentes.	60 dias úteis, contados da data de recebimento da Ordem de Fornecimento.	de entrega dos produtos, sendo a contagem do prazo iniciando-se após a emissão da Ordem de Serviço(s).

2.9. **Requisitos de segurança e privacidade:**

2.9.1. Todos os serviços suportados pela CONTRATADA devem seguir as normas de Segurança da Informação da Infra S.A., guias e normativos da Secretaria de Governo Digital, assim como eventuais outras normas de segurança que se apliquem, ainda que editadas futuramente, em especial a Lei nº 13.709, de 14 de agosto de 2018: dispõe sobre a Lei Geral de Proteção de Dados Pessoais – LGPD.

2.9.2. Implementação de mecanismos de segurança avançados, como criptografia de ponta a ponta, autenticação multifator e segregação de acesso, garantindo a confidencialidade e a integridade dos dados operacionais.

2.9.3. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto e informação de que tomar conhecimento em razão da execução do objeto do Contrato.

2.9.4. Providenciar assinatura do Termo de Sigilo e Confidencialidade, conforme modelo a ser estabelecido, pelo representante legal da empresa.

2.10. **Requisitos sociais, ambientais e culturais:**

2.10.1. Os preceitos normativos que consubstanciam a promoção do desenvolvimento nacional sustentável no âmbito das contratações pela Administração Pública (IN SLTI/MPOG nº 01/2010 c/c Lei nº 13.303/2016, e Decreto 7.746/2012) serão observados pelas partes CONTRATANTES de forma que:

a) O objeto das relações contratuais entabuladas cause o menor impacto possível sobre recursos naturais;

b) Preferência para materiais, tecnologias e matérias-primas de origem local;

c) Maior eficiência na utilização de recursos naturais;

d) Maior geração de empregos, preferencialmente com mão de obra local;

e) Maior vida útil e menor custo de manutenção do bem;

f) Uso de inovações que reduzam a pressão sobre recursos naturais; e

g) Origem ambientalmente regular dos recursos naturais utilizados nos bens e serviços.

2.10.2. A CONTRATADA deverá assegurar a viabilidade técnica e o adequado tratamento do impacto ambiental específicos, inclusive:

a) origem sustentável dos recursos naturais utilizados nos bens e serviços;

b) adotar práticas de gestão que garantam os direitos trabalhistas e o atendimento às normas internas e segurança e medicina do trabalho para seus empregados;

c) administrar situações emergenciais de acidentes com eficácia, mitigando os impactos aos empregados, colaboradores, usuários e ao meio ambiente;

d) conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e à saúde dos trabalhadores e envolvidos na prestação dos serviços;

e) respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;

f) orientar seus empregados para a destinação dos resíduos recicláveis descartados aos devidos coletores de resíduos recicláveis.

2.11. **Requisitos de arquitetura tecnológica:**

2.11.1. A solução deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD, OKTA, JumpCloud entre outros.

2.11.2. A solução deve permitir a integração com diferentes plataformas de segurança via API.

2.11.3. Todos os componentes da solução devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

2.11.4. Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

2.11.5. A solução deve suportar a comunicação dos componentes instalados por meio de um proxy web.

2.11.6. O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

2.11.7. A solução deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

2.11.8. A solução deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

2.11.9. Todos os produtos de segurança que não possuírem integração direta, devem poder ser integrados por meio soluções de correlacionamento de eventos (SIEM), permitindo a integração com produtos não homologados.

2.11.10. A solução deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.

2.11.11. A solução deve permitir avaliar as capacidades de defesa da organização contra táticas, técnicas e procedimentos utilizados por grupos criminosos conhecidos.

2.11.12. A solução deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.

2.11.13. O portfólio de ataques da solução deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS, Microsoft DRAPE e NIST.

2.11.14. As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.

2.11.15. A solução deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:

2.11.16. Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:

I - Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.

II - Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo estes realizar a

descoberta de hosts vulneráveis e simular a proliferação para eles através de técnicas utilizando protocolos tais como SMB.

III - Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.

IV - Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.

V - MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

2.11.17. Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

I - Phishing: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção de ataques de phishing, acessando IPs e URLs reais associados a ataques de phishing identificados recentemente.

II - Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.

III - C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.

IV - Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.

V - Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.

VI - Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares que simulam o comportamento de worms, trojans e ransomware.

2.11.18. Para validação do vetor de email gateway a plataforma deve oferecer simulações de ataque para:

I - Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

II - Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

III - Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente

IV - Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser

realizada de forma segura sem gerar impactos ao ambiente.

V - Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

VI - Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

2.12. **Requisitos de projeto e de implementação:**

2.12.1. Os serviços deverão observar integralmente os requisitos de implantação, conforme a seguir:

2.12.1.1. Planejamento e design da instalação: A CONTRATADA deverá fornecer um plano detalhado de instalação e design, realizando reuniões técnicas conforme necessário. com o objetivo de ser apresentada objetivamente ao Projeto de Serviços Gerenciados de Segurança proposto pela Infra S.A., devendo sinalizar quaisquer inviabilidades ou ajustes necessários, propondo as alternativas e/ou melhorias no projeto com o foco em viabilizar a implementação. Para cada reunião, deverão ser elaboradas atas para registro dos pontos abordados e consentimento global, que subsidiarão a próxima fase da dinâmica de execução.

2.12.1.2. A CONTRATADA deverá entregar Documento de Instalação tomando como base todo o projeto apresentado pela Infra S.A. e as abordagens registradas nas atas de reunião, contendo o projeto e layout de conexão e proposta de configuração dos equipamentos; também deve conter plano de testes para validação do funcionamento pós -execução. Esse documento deverá ser entregue para avaliação e aprovação da Infra S.A para execução dos serviços.

2.12.1.3. Execução dos serviços de instalação e configuração: A CONTRATADA deverá garantir a instalação e configuração da solução seguindo o Documento de Instalação e as Boas Práticas disponibilizadas pelos fabricantes da solução, devidamente aprovado pela Infra S.A. As janelas de manutenção para execução dos serviços serão definidas pela Infra S.A., podendo ocorrer em dias e horários que não coincidam com os horários comerciais tais como finais de semana, feriados e em janelas noturnas/madrugada.

2.12.1.4. A pretensa contratação da solução de tecnologia da informação deve prever o fornecimento e instalação de todos os insumos necessários para operacionalização da solução adquirida sem gerar custos adicionais para a Infra S.A.

2.12.1.5. Realização do plano de testes: A CONTRATADA deverá realizar o plano de testes definido previamente, executando a correção de eventuais problemas encontrados, conforme cronograma aprovado de implantação.

2.12.1.6. Realização da transferência de conhecimento e operação assistida: A CONTRATADA deverá fornecer documentação e transferência de conhecimento necessários para a equipe técnica da Infra S.A. sobre a solução e suas características gerais, para a equipe técnica da Infra S.A que indicará os participantes, registrando em ata a data de realização da sessão, o conteúdo abordado e a assinatura dos participantes, devendo ser entregue ao final dessa fase.

2.12.1.7. Também deverá, após a implantação da solução, acompanhar os primeiros 30 (trinta) dias corridos o funcionamento da solução para correção imediata de eventuais problemas e, se for o caso, para realização de melhorias identificadas após a implantação. Por fim, deverá ainda realizar operação assistida nas primeiras 24 (vinte e quatro) horas corridas pós implementação da solução, corrigindo, quando necessário, eventuais problemas decorrentes da execução.

2.12.1.8. Elaboração e entrega da documentação (AS-BUILT) do ambiente instalado: A

CONTRATADA deverá entregar à Infra S.A. toda documentação do ambiente instalado, descrevendo em detalhes todos os aspectos de configuração da solução. Passados os 30 (trinta) primeiros dias corridos da implantação da solução a CONTRATADA deverá disponibilizar suporte técnico.

2.12.1.9. Monitoramento contínuo do ambiente de TI: utilizando tecnologias de inteligência artificial e machine learning para detectar e responder a incidentes. Manutenção preventiva e corretiva para garantir o funcionamento ininterrupto da solução. E Geração de relatórios regulares e análises de segurança para informar sobre o estado da segurança e a eficácia das medidas implementadas.

2.13. **Requisitos de implantação:**

2.13.1. Emissão da Ordem de Serviço - OS - 5 (cinco) dias úteis da Reunião Inicial.

2.13.2. Apresentação do Plano de Implantação - 10 (dez) dias corridos da Reunião Inicial.

2.13.3. Validação do Plano de Implantação - 5 (cinco) dias úteis, contados a partir de seu recebimento

2.13.4. Aprovação Plano de Implantação - 5 (cinco) dias úteis, contados da validação

2.13.5. Realização da instalação e configuração da solução - 60 (sessenta) dias corridos da data de entrega dos produtos, sendo a contagem do prazo iniciando-se após a emissão da Ordem de Serviço(s).

2.13.6. Realização de repasse de conhecimento da Solução - Iniciado em até 5 (cinco) dias úteis após conclusão do item 3.1.8.5. (Essa etapa pode ser remarcada a critério da Infra S.A., sem prejuízo às demais etapas.)

2.13.7. Sinalização da conclusão de implantação da solução - 10 (dez) dias corridos após conclusão da implantação plena da solução

2.13.8. Emissão de Termo de Recebimento Provisório - Verificação da conclusão da implantação da solução - 5 (cinco) dias úteis após o recebimento item 3.1.8.7.

2.13.9. Emissão de Termo de Recebimento Definitivo - 10 (dez) dias úteis contados da emissão do TRP.

2.14. **Requisitos de garantia técnica e manutenção:**

2.14.1. Oferta de garantia técnica de no mínimo 24 (vinte e quatro) meses para todos os componentes da solução, incluindo hardware, software e atualizações.

2.14.2. Adoção de Acordos de Nível de Serviço (SLA) específicos para a Infra SA, com prazos máximos de resposta e solução de incidentes que atendem às necessidades críticas de operação.

2.14.3. Atualizações periódicas de funcionalidades e bases de dados, priorizando a adaptação às novas ameaças relacionadas à infraestrutura de transporte e logística.

2.15. **Requisitos de experiência profissional:**

2.15.1. Os serviços de suporte e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

2.15.2. A CONTRATADA deverá apresentar representante técnico especialista, comprovadamente habilitado na(s) solução(ões), para atuar como “Líder Técnico” para o tratamento de todas as questões administrativas e técnicas referentes à(s) solução(ões) adquirida(s), incluindo a entrega e instalação dos bens adquiridos.

2.15.3. A CONTRATADA deverá apresentar técnicos encarregados dos serviços ao ambiente da CONTRATANTE, com certificações técnicas vigentes na solução ofertada, reconhecida pelo

fabricante, que tenham validade enquanto durar o período de garantia contratual, a fim de garantir que a instalação, configuração inicial, atualização tecnológica bem como o suporte técnico durante o prazo de garantia de qualidade só poderão ser realizados por profissionais certificados com certificações reconhecidas pelo fabricante, nos componentes da solução ofertada.

2.16. **Requisitos de formação da equipe:**

2.16.1. Não serão exigidos requisitos de formação de equipe para a presente contratação.

2.17. **Requisitos de metodologia de trabalho:**

2.17.1. Os serviços de suporte técnico em garantia deverão seguir as melhores práticas preconizadas pelo ITIL - Information Technology Infrastructure Library.

2.17.2. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

2.17.3. A OS indicará o serviço, a quantidade e a localidade na qual deverão ser prestados.

2.17.4. O Contratado deve fornecer meios para contato e registro de ocorrências com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica.

2.17.5. A execução do serviço dever ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

2.18. **Requisitos de segurança da informação e privacidade:**

2.18.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela Contratante a tais documentos.

2.18.2. A Contratada deverá observar a Política de Segurança da Informação e demais as normas de segurança da informação da Contratante, disponíveis em seu site.

2.18.3. Na hipótese de, em razão da execução do presente Contrato, a Contratada realizar operações de tratamento de dados pessoais relacionados à Contratante, a Contratada declara estar ciente e concorda com as disposições constantes no futuro Contrato.

2.18.4. Demais requisitos de segurança e privacidade serão minudenciados no futuro Contrato.

2.19. **Demais requisitos aplicáveis:**

2.19.1. **Requisitos de subscrição e licenciamento:**

2.19.2. Suporte, garantia e funcionalidades descritas neste ETPC, que necessitem de licenciamento, deverão ser entregues para um período mínimo de 24 (vinte e quatro) meses, podendo a critério da CONTRATANTE, ser prorrogado até o limite de 60 (sessenta) meses;

2.19.3. A solução deve possuir garantia, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento e demais softwares e das assinaturas necessárias para funcionamento das funcionalidades;

2.19.4. Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional, firmware, software da solução para obter novas funcionalidades e correção de bugs;

2.19.5. Todas as funcionalidades adquiridas na solução que podem compreender hardware, software e serviços devem operar conforme disposto neste ETPC durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares, softwares e serviços para esse período.

2.19.6. **Requisitos de segurança:**

2.19.6.1. A CONTRATADA deverá obedecer aos procedimentos operacionais relacionados à segurança física, patrimonial e de acesso adotados pela CONTRATANTE.

2.19.7. **Requisito de sustentação:**

2.19.7.1. Todas as ferramentas fornecidas como parte das soluções devem contar com serviços plenos de sustentação, conforme a seguir:

- A sustentação, administração, operação, suporte técnico e atualização das ferramentas fornecidas pela contratada, e qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos serão serviços de natureza continuada de responsabilidade da contratada;
- Para cada uma delas, devem ser fornecidos os serviços de suporte técnico e de atualização oficiais e prioritários do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços envolvidos, que devem estar contratados e disponíveis a partir da implantação da respectiva ferramenta e, daí em diante, durante toda a vigência do contrato;
- A contratada deve comprovar um nível de parceria oficial amplo e prioritário junto ao fabricante, tal que permita amplo e irrestrito acesso aos recursos e serviços de apoio técnico e de acesso à plenitude de capacidades e efetividade das ferramentas, prestados diretamente pelo fabricante, como centros e laboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis;
- As ferramentas que forem de uso exclusivo da Infra S.A., ou que sejam assim demandadas pelo modelo de negócios do fabricante, devem ser devidamente licenciadas ou subscritas em nome da Infra S.A., devendo a contratada apresentar a devida comprovação para que sejam iniciados os pagamentos dos respectivos itens de serviço.

2.19.8. **Requisitos de gestão e relatório:**

2.19.8.1. A solução deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

2.19.8.2. A console deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

2.19.8.3. A console deve fornecer uma visão global dos itens que foram identificados.

2.19.8.4. A solução deve possuir uma interface amigável em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

2.19.8.5. Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

2.19.8.6. A solução deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

2.19.8.7. A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

2.19.8.8. A console deve fornecer uma guia para download e gestão dos agentes implementados.

2.19.8.9. A Contratada deverá apresentar mensalmente, até o 5º (quinto) dias úteis do mês subsequente, relatório técnico sobre a condições de testes realizados na infraestrutura da Infra S

2.19.9. **Requisitos adicionais:**

2.19.9.1. Integração da solução com os sistemas corporativos já utilizados pela Infra SA, como plataformas de gestão operacional e logística, garantindo maior sinergia entre as ferramentas.

2.19.9.2. Fornecimento de relatórios estratégicos customizáveis, com análises previstas sobre ameaças monitoradas que possam impactar o setor ferroviário, logístico e de infraestrutura da organização.

2.19.9.3. Disponibilidade de dashboards interativos, permitindo o acompanhamento em tempo real de métricas e indicadores-chave de segurança cibernética.

2.19.9.4. Adesão aos padrões internacionais de segurança e melhores práticas de TI, como ISO 27001, NIST e COBIT, garantindo a confiabilidade da solução.

2.20. **Identificação de padrões mínimos de qualidade e desempenho do serviço:**

2.20.1. Para garantir a eficácia e a confiabilidade da solução de serviços de proteção contra-ataques cibernéticos, é essencial estabelecer padrões mínimos de qualidade e desempenho. Esses padrões servirão como critérios para avaliar a prestação do serviço e assegurar que ele atenda às necessidades de segurança da Infra S.A. Os principais padrões mínimos incluem:

2.20.1.1. Disponibilidade e Confiabilidade:

- Uptime - A solução deve garantir uma disponibilidade mínima de 99,9% assegurando que os serviços estejam operacionais e acessíveis em quase todo o tempo - Redundância - Implementar mecanismos de redundância, para evitar interrupções no serviço, incluindo backups regulares e failover automático;

2.20.1.2. Eficiência na Detecção e Resposta:

- Tempo de Detecção (MTTD) - O tempo médio para detectar uma ameaça deve ser inferior a 5 minutos - Tempo de Resposta (MTTR) - O tempo médio para responder e mitigar uma ameaça deve ser inferior a 30 minutos.

2.20.1.3. Cobertura Abrangente:

- Escopo de Proteção - A solução deve cobrir todas as camadas de segurança, incluindo rede, endpoint, aplicativos e dados - Atualizações de Segurança - Atualizações regulares e automáticas para garantir a proteção contra as ameaças mais recentes.

2.20.1.4. Precisão e Redução de Falsos Positivos:

- Taxa de Falsos Positivos - A solução deve manter uma taxa de falsos positivos inferior a 2% minimizando alertas desnecessários e garantindo a precisão na detecção de ameaças reais.

2.20.1.5. Capacidade de Escalabilidade:

- Escalabilidade - A solução deve ser capaz de escalar conforme o crescimento da infraestrutura da Infra S.A. suportando um aumento no volume de dados e usuários sem perda de desempenho.

2.20.1.6. Relatórios e Transparência:

- Relatórios Detalhados - Fornecimento de relatórios detalhados e regulares sobre o desempenho do serviço, incidentes detectados e ações tomadas - Transparência - Acesso transparente às métricas de desempenho e logs de atividades para auditorias e conformidade.

2.20.1.7. Suporte Técnico e Manutenção:

- Suporte 24/7 - Disponibilidade de suporte técnico especializado 24 horas por dia, 7 dias por semana, para resoluções de problemas e assistência emergencial - Manutenção Proativa - Realização de manutenção proativa e preventiva para garantir o funcionamento contínuo e eficiente da solução.

2.20.1.8. Conformidade com Regulamentações:

- Conformidade Legal - A solução deve estar em conformidade com todas as regulamentações e normas aplicáveis, com LGPD e o Marco Civil da Internet - Certificações de Segurança - Possuir certificações reconhecidas de segurança cibernéticas, como ISO 27001, para garantir a aderência às melhores práticas do setor.

2.20.1.9. Treinamento e Capacitação:

- Capacitação Contínua - Oferecer programas de treinamento contínuo para a equipe de segurança da Infra S.A, garantindo que estejam atualizados com as últimas técnicas e práticas de defesa cibernética.

2.20.2. Estes padrões mínimos de qualidade e desempenho são fundamentais para assegurar que a solução de proteção contra-ataques cibernéticos forneça uma defesa robusta, eficiente e confiável, alinhada com as necessidades estratégicas e operacionais da Infra S.A.

2.21. Para a presente contratação será elaborado Termo de Referência com os elementos necessários e suficientes, com nível de precisão adequado para definir e dimensionar os serviços, que assegure a viabilidade técnica e o adequado tratamento do impacto ambiental do empreendimento, se for o caso, de modo a possibilitar a avaliação do custo dos serviços e a definição dos métodos e do prazo de execução.

3. ANÁLISE COMPARATIVA DAS SOLUÇÕES

3.1. A análise comparativa de soluções, considera, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação. As alternativas refletem diferentes abordagens para atender às necessidades de manutenção preventiva e corretiva com reposição de peças do datacenter, cada uma com seus próprios méritos e limitações.

3.2. **As necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:**

3.2.1. Conforme tabela a seguir, foram encontradas necessidades similares em outros órgãos/entidades da Administração Pública e as soluções adotadas:

Órgão	Objeto	Modalidade	Fonte de Pesquisa
STF - Supremo Tribunal Federal	Serviços especializados para fornecimento de subscrições para solução de detecção e resposta estendida para incidentes de segurança cibernética	Pregão Eletrônico nº 90005/2024	www.gov.br/compras/pt-br

UEG - Universidade Estadual de Goiás	Segurança Cibernética com inclusão de uso de licença NGWF	Pregão Eletrônico nº 23/2023	sislog.go.gov.br/PainelAquisicao
Prefeitura Municipal de Vila Velha - ES	Soluções de Segurança para Perímetro de rede e defesa Cibernética e contratação de SOC.	Registro de Preços nº 106/2024	https://diariooficial.vilavelha.es.gov.br

3.3. **As alternativas do mercado:**

Item	Descrição	Produto	Fabricante
1	Serviços especializados para fornecimento de subscrições para solução de detecção e resposta estendida para incidentes de segurança cibernética	BAS	Keysigth, Picus, AttacklQ, SafeBreach, Cymulate, Pentera, XC Cyber e Mandiant.

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

3.4.1. Não se aplica ao objeto da pretensa contratação.

3.5. **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:**

3.5.1. Não se aplica ao objeto da pretensa contratação.

3.6. **As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual:**

3.6.1. Não se aplica ao objeto da pretensa contratação.

3.7. **Os diferentes modelos de prestação do serviço:**

3.7.1. Os modelos de prestação de serviços desta contratação são:

Modelo	Descrição	Características	Vantagens	Desvantagens
Modelo Gerência de Segurança e Serviços (MMS)	Neste modelo, um provedor de serviços gerencia completamente a simulação de ataques cibernéticos. Isso inclui a configuração, execução e análise dos testes de simulação.	• Configuração e Implementação; • Monitoramento contínuo • Execução de Testes de Simulação; • Análise e Relatórios; • Atualizações e Manutenção.	Monitoramento contínuo, expertise especializada, e relatórios detalhados sobre vulnerabilidades e recomendações de mitigação	Riscos de conformidade e desafios na comunicação e coordenação especialmente em situações de emergências

Serviços baseados em assinaturas	As organizações pagam uma taxa de assinatura para acessar as plataformas, incluindo as de detecção e análise de ameaças	• Acesso contínuo; • Atualizações regulares; • Escalabilidade e flexibilidade de Pagamento	Custos previsíveis, acesso a atualizações contínuas, suporte técnico especializado e escalabilidade.	Dependência do provedor, custo elevado, limitação de personalização e riscos de conformidade

3.8. **Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes:**

3.8.1. Para o presente estudo, utilizou-se as soluções constantes no item 3.12.

3.9. **A possibilidade de aquisição na forma de bens ou contratação como serviço:**

3.9.1. A necessidade desta contratação pode ser atendida pela contratação de serviços.

3.10. **A ampliação ou substituição da solução implantada:**

3.10.1. Não se aplica ao objeto da pretensa contratação.

3.11. **As diferentes métricas de prestação do serviço e de pagamento:**

3.11.1. Não se aplica ao objeto da pretensa contratação.

3.12. **Identificação das Soluções:**

3.12.1. Foram avaliadas soluções implementadas em outros órgãos ou instituições públicas, tendo sido realizada a análise entre as soluções disponíveis, a saber:

Solução	Descrição
S1	Utilização de equipe e de estrutura interna
S2	Contratação e implantar um SOC interno
S3	Contratações apartadas do objeto que separe o fornecimento de ferramentas e tecnologias do fornecimento dos serviços e equipe técnica.
S4	Contratação de solução para validação de segurança contínua, com serviços gerenciados de segurança cibernética (*Managed Security Services* – MSS)
S5	Contratação de softwares livres gratuitos.

3.12.2. A análise das soluções para a contratação de serviços de monitoramento e segurança cibernética apresentou diferenças substanciais entre as abordagens avaliadas, considerando aspectos de custo, eficiência, implementação e alinhamento, conforme segue:

Solução	Descrição	Vantagens	Desvantagens

S1	Utilização de equipe e de estrutura interna	• Controle direto sobre as operações e monitoramento. • Conhecimento das especializações do ambiente interno pela própria equipe. • Potencial redução de custos com serviços externos a longo prazo.	• Elevado custo inicial para treinamento e aquisição de ferramentas especializadas. • Demandas por contratação e capacitação contínua de profissionais em segurança cibernética. • Limitação de recursos internos para atender à complexidade do monitoramento em ambientes como Deep e Dark Web. • Dificuldade em manter a operação atualizada frente à rápida evolução das ameaças cibernéticas. • Desafios técnicos operacionais
S2	Contratação e implantar um SOC interno	• Capacidade de personalizar as operações de monitoramento e responder de acordo com as necessidades específicas da Infra SA • Maior controle e confidencialidade das informações sensíveis. • Operação 24/7 com foco exclusivo na segurança da organização.	• Altíssimo custo inicial para instalação de infraestrutura física, aquisição de ferramentas e contratação de especialistas. • Complexidade técnica e operacional para manter o SOC atualizado e funcional. • Demanda por um quadro de profissionais altamente reforçados e treinamento constante. • Longevidade do retorno do investimento em relação ao dinamismo das ameaças cibernéticas e novas tecnologias. • Custo proibitivo e complexidade

S3	Contratação apartada do objeto que separe o fornecimento de ferramentas e tecnologias do fornecimento dos serviços e equipe técnica.	• Permite a aquisição de ferramentas de alta tecnologia sem comprometer o orçamento com serviços completos. • Flexibilidade para selecionar fornecedores diferentes para ferramentas e equipes técnicas. • Potencial redução de custos ao adquirir apenas as tecnologias ou serviços específicos necessários.	• Desafios de integração entre as ferramentas e os serviços contratados separadamente. • Aumento da complexidade na gestão de múltiplos contratos e fornecedores. • Risco de falta de sinergia entre equipes técnicas e as ferramentas adquiridas. • Menor eficiência na operação contínua devido à fragmentação dos serviços. • **Fragmentação operacional** , dificultando a integração entre ferramentas adquiridas e os serviços técnicos contratados separadamente. • Maior complexidade administrativa na gestão de múltiplos contratos e fornecedores. • Possível comprometimento da eficiência operacional devido à falta de sinergia entre ferramentas e equipes técnicas, impactando a qualidade da resposta às ameaças.
	Contratação de solução para	• **Abordagem integrada** que combina ferramentas tecnológicas avançadas, validação contínua de segurança e suporte especializado. • Monitoramento e resposta a ameaças cibernéticas em regime 24 horas por dia, 7 dias por semana, sem necessidade de infraestrutura própria ou equipe interna dedicada. • Atualizações automáticas e contínuas para acompanhar a evolução das ameaças, garantindo a eficácia das	• Dependência de terceiros para execução e monitoramento, exigindo

S4	validação de segurança contínua, com serviços gerenciados de segurança cibernética, (Managed Security Services – MSS)	empregadas ferramentas. • Custos mais previsíveis e escaláveis, alinhados ao planejamento orçamentário da Infra SA • Acesso a expertise de ponta e tecnologias avançadas, sem necessidade de investimentos importantes em capacitação interna. • Possibilidade de integração com sistemas internos existentes, garantindo sinergia e eficiência na operação. • Redução significativa do tempo de resposta a incidentes, com impacto positivo na continuidade operacional e proteção de ativos críticos.	contratos robustos com SLAs bem definidos para mitigar riscos. • Necessidade de supervisão e auditorias contínuas para garantir a qualidade e o cumprimento dos serviços prestados aos objetivos estratégicos da Infra SA.

S5	Contratação de softwares livres gratuitos.	• Custo reduzido ou nulo para aquisição de licenças: A utilização de software livre elimina ou minimiza os gastos com licenciamento, possibilitando economia inicial significativa. • Flexibilidade e customização: Softwares livres frequentemente permitem ajustes e personalizações para atender às necessidades específicas da Infra SA • Comunidade ativa: Muitos softwares gratuitos contam com comunidades globais que oferecem suporte, atualizações e melhorias contínuas, sem custos adicionais. • Independência de fornecedores: Reduz a dependência de contratos específicos, permitindo maior autonomia tecnológica. • Aderência a padrões abertos: Facilita a interoperabilidade com outros sistemas e tecnologias.	• Capacidade limitada de suporte técnico: O suporte geralmente depende de comunidades ou de discussões de serviço externo, o que pode comprometer uma resposta a incidentes críticos. • Falta de garantia de atualizações rápidas e de segurança: Sem contratos de suporte formalizados, pode haver demora na correção de vulnerabilidades, comprometendo a segurança. • Riscos de compatibilidade: Integração com sistemas existentes pode ser complexa, especialmente em ambientes corporativos como o da Infra SA • Dependência de equipe interna ou de terceiros para manutenção: Embora os softwares sejam gratuitos, a implementação e gestão desabilitam expertise técnica interna ou contratação de especialistas, gerando custos indiretos. • Responsabilidade por validação de segurança contínua: Ferramentas livres não podem incluir validação contínua ou monitoramento em tempo real, exigindo soluções complementares

3.13. **Análise Comparativa:**

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	S1			X
	S2			X
	S3			X
	S4	X		
	S5			X

Requisito	Solução	Sim	Não	Não se Aplica
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas em padrões de governo ePing, eMag, ePWG?	S1			X
	S2	X		
	S3			X
	S4	X		
	S5	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	S1			X
	S2			X
	S3			X
	S4			X
	S5			X

3.14. 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, não se aplica ao objeto da presente contratação.

3.15. **Registro de Soluções Consideradas Inviáveis**

3.15.1. Como análise entre os prós e contras de cada uma das soluções conclui-se que:

3.15.1.1. As análises mostram que **S1, S2, S3 e S5 são inviáveis** para atender às necessidades da Infra SA, seja pelo alto custo, pela complexidade de implementação ou pela ineficiência operacional e administrativa.

3.16. **Registro de Solução Considerada Viável:**

3.16.1. A **Solução 4 (Contratação de solução para validação de segurança contínua, com**

serviços gerenciados de segurança cibernética (*Managed Security Services* – MSS)) é a opção mais viável, pela conveniência, validação contínua de segurança, serviços gerenciados e acesso a tecnologias de ponta sem os altos custos de infraestrutura e operação interna. Além disso, a solução no modelo MSS oferece flexibilidade e agilidade para proteger os ativos críticos da Infra SA frente à evolução das ameaças cibernéticas. Considerando, ainda, que o mercado conta com fornecedores que ofereçam integração, relatórios personalizados e garantia de cumprimento de SLAs. Isso garantirá proteção eficiente, custo-benefício e alinhamento aos objetivos estratégicos da organização.

3.16.2. Outrossim, a **Solução 4** se destaca como a opção capaz de oferecer uma abordagem eficiente, escalável e compatível com as necessidades estratégicas da Infra SA, proporcionando os seguintes benefícios:

I - Atendimento integral às demandas críticas de segurança cibernética: A MSS oferece validação contínua de segurança, monitoramento em tempo real e resposta ágil a incidentes. E, permite o monitoramento de ambientes sensíveis, como Deep e Dark Web, que são essenciais para antecipar ameaças relevantes ao setor de infraestrutura.

II - Custo-benefício: Apesar de envolver custos recorrentes, o modelo de contratação oferece previsibilidade financeira, evitando os elevados custos iniciais de outras soluções. Não exige investimentos em infraestrutura própria, contratação de especialistas ou manutenção interna, reduzindo os custos indiretos.

III - Expertise e tecnologia de ponta: A MSS garante acesso a ferramentas avançadas, atualizadas continuamente para lidar com ameaças emergentes, sem a necessidade de investimento direto pela Infra SA. O suporte especializado 24 horas por dia, 7 dias por semana garante agilidade na identificação e mitigação de riscos.

IV - Escalabilidade e flexibilidade: A solução pode ser ajustada conforme o crescimento das demandas da Infra SA, integrando-se aos sistemas existentes e permitindo expansões futuras.

V - Mitigação de riscos: Ao contar com um serviço especializado, a Infra SA reduz sua exposição a falhas operacionais e riscos associados à gestão interna da segurança cibernética.

4. ANÁLISE COMPARATIVA DE CUSTOS

4.1. A presente seção registra comparação de Custos Totais de Propriedade para a solução técnica e funcionalmente viável, nos termos do inciso III do art. 11. da IN SGD/ME nº 94/2022. Destaca-se também que a identificação dos custos totais das soluções pautou-se pela obtenção de preços, conforme parâmetros descritos no art. 9º, da Resolução Normativa - INFRASA Nº 9/2023/DIREX-INFRASA/CONSAD-INFRASA/AG-INFRASA.

4.2. Dentre as soluções apresentadas, somente a Solução S4 atende à demanda na sua totalidade referente aos requisitos essenciais.

4.3. A memória de cálculo que referencia os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados, encontra-se no Anexo "Documentação Pesquisa de Mercado_FORNECEDORES (9138141), "Documentação Pesquisa de Mercado GOVERNO (9119867)" e "Planilha MetodologiaCGU_Solução CibernéticaV2.2 (9142216)" no processo apartado e amparado pelo Art. 28 da Lei 13.303/2016 - Sigilo aos orçamentos estimados nº 50050.008175/2024-23.

4.4. Análise Comparativa de Custos (TCO):

Solução Viável 4
Descrição:
Solução S4: Contratação de solução para validação de segurança contínua, com serviços gerenciados de segurança cibernética (*Managed Security Services* – MSS)

Custo Total:
Conforme item 4.3

4.4.1. A análise comparativa de custos está detalhada no documento "Anexo I Análise Comparativa de Custos (9143329)", localizado em processo apartado e amparado pelo Art. 28 da Lei 13.303/2016 - Sigilo aos orçamentos estimados.

4.5. **Mapa Comparativo dos Cálculos:**

4.5.1. Os resultados estão apresentados no Mapa Comparativo de Preços (9116461) , localizado em em processo apartado e amparado pelo Art. 28 da Lei 13.303/2016 - Sigilo aos orçamentos estimados.

5. DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA COMO UM TODO

5.1. A Solução S4 - Contratação de solução para validação de segurança contínua, com serviços gerenciados de segurança cibernética (*Managed Security Services* – MSS)) é a opção escolhida, por ter sido considerada viável tecnicamente e economicamente para o período de 24 (vinte e quatro) meses.

5.2. O rol de itens e subitens de serviços é conforme a seguir:

5.2.1. Implantação:

5.2.1.1. Levantamento e avaliação inicial da infraestrutura e dos ativos de TIC

5.2.1.2. Capacitação

5.2.2. Governança e gestão de segurança de TIC:

5.2.2.1. Serviços estratégicos de governança, risco e conformidade (GRC)

5.2.2.2. Definição de controles, salvaguardas e remediações

5.2.3. Monitoramento, detecção e resposta gerenciados de segurança:

5.2.3.1. Centro de operações de segurança (SOC), equipe de tratamento e resposta a incidentes (ETIR) e gerenciamento e análise de eventos e informações de segurança (SIEM)

5.2.3.2. Orquestração e automação e resposta (SOAR)

5.2.3.3. Proteção contra riscos digitais (DRP)

5.2.4. Gestão de vulnerabilidades e testes de segurança:

5.2.4.1. Gestão contínua de vulnerabilidades e de exposição a ameaças baseada em riscos

5.2.4.2. Testes de segurança automatizados (BAS)

5.2.5. Identidade e acesso:

5.2.5.1. Diagnóstico e avaliação de governança de identidade (IGA) e gestão de acessos (AM)

5.2.5.2. Serviços técnicos especializados, sob demanda

5.2.5.3. Testes de invasão (PenTest)

5.3. Esta composição da solução atende integralmente e está totalmente aderente aos requisitos, bem como se mostrou viável e adequada tanto em consultas ao Gartner quanto em análises de prospecção de mercado por várias empresas e seu rol e segmentação de produtos e serviços ofertados.

6. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

6.1. A quantidade prevista a ser contratada:

Grupo	Item	Descrição	Quantidade	Unidade

1	1	Serviços de Simulação de Violação e Ataques Cibernéticos	1	Unidade

6.2. **Memória de cálculo e os documentos que dão suporte:**

6.2.1. A memória de cálculo das estimativas das quantidades está detalhada na Documentação Ambiente Computacional - INFRA S.A. (9138049).

6.3. **Interdependência com outras contratações:**

6.3.1. Não se verifica interdependência com outras contratações para a viabilidade e contratação desta demanda.

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

7.1. A memória de cálculo do custo total da contratação e os documentos que dão suporte encontram-se no documento Anexo I Análise Comparativa de Custos (9143329), constante de processo sigiloso apartado (50050.008175/2024-23).

7.2. **Justificativa técnica da escolha da solução:**

7.2.1. A contratação de uma solução de simulação de ataques cibernéticos é uma decisão estratégica e técnica fundamentada nas necessidades operacionais e de segurança da Infra S.A. A seguir, apresentamos as razões que justificam a escolha desta solução:

7.2.1.1. Necessidade de Modernização da Infraestrutura: A atual infraestrutura tecnológica da Infra S.A. requer modernização para atender à crescente demanda por eficiência e segurança. A aquisição de uma solução de simulação de ataques cibernéticos permite a atualização e a adequação às melhores práticas do mercado, garantindo que a infraestrutura esteja preparada para enfrentar ameaças modernas.

7.2.1.2. Proteção Contra Ameaças Cibernéticas: Com o aumento das ameaças cibernéticas, a adoção de uma solução robusta de segurança é imprescindível. A solução de simulação de ataques cibernéticos inclui mecanismos avançados de detecção e bloqueio de ataques, proteção de aplicativos web e avaliações contínuas de vulnerabilidades. Isso proporciona uma defesa proativa e eficaz contra os riscos associados à segurança da informação.

7.2.1.3. Gerenciamento Eficaz de Acessos: A implementação de soluções que viabilizam o acesso à rede com base na identidade e em políticas de segurança é crucial para mitigar riscos de acessos não autorizados. A gestão de privilégios e a proteção dos recursos críticos são fundamentais para garantir a integridade e a confidencialidade dos dados.

7.2.1.4. Conformidade com Regulamentações: A escolha da solução também visa assegurar maior conformidade com as regulamentações pertinentes, especialmente em relação aos requisitos de segurança cibernética e privacidade de dados, como a LGPD. Isso não apenas minimiza riscos legais, mas também fortalece a confiança dos cidadãos na gestão dos dados públicos.

7.2.1.5. Infraestrutura de Rede Segura e Escalável: A solução proporciona uma infraestrutura de rede com alta disponibilidade e escalabilidade, essencial para suportar o crescimento da demanda por serviços. A capacidade de atender às necessidades de mobilidade e conectividade de dispositivos sem fio é um diferencial significativo em um cenário tecnológico em constante evolução.

7.2.1.6. Eficiência Operacional e Redução de Custos: A automação e o gerenciamento centralizado simplificam as operações de segurança, reduzindo o tempo de resposta a incidentes. A validação contínua das ferramentas e a simulação de ataques permitem identificar e corrigir vulnerabilidades antes que sejam exploradas, diminuindo o risco de incidentes

dispendiosos.

7.2.1.7. Modelos de Prestação de Serviços: A solução de simulação de ataques cibernéticos pode ser fornecida através de diferentes modelos de prestação de serviços, como serviços gerenciados (MSS), serviços baseados em assinatura, serviços de consultoria e implementação, e serviços de suporte e manutenção. Cada modelo oferece benefícios específicos, como monitoramento contínuo, custos previsíveis, suporte técnico especializado e escalabilidade, permitindo que a Infra S.A. escolha a abordagem que melhor se adapta às suas necessidades.

7.2.1.8. Alternativas de Mercado: Existem várias alternativas de mercado para soluções de simulação de ataques cibernéticos, incluindo plataformas de fornecedores renomados como Keysigth, Picus, AttacklQ, SafeBreach, Cymulate, Pentera, XC Cyber e Mandiant. Essas soluções oferecem uma variedade de funcionalidades e abordagens para proteger contra ameaças cibernéticas, permitindo que a Infra S.A. escolha a solução que melhor se adapta às suas necessidades específicas de segurança e infraestrutura.

7.2.1.9. A aquisição da pretensa solução é essencial para assegurar os requisitos de confidencialidade, disponibilidade e integridade das informações custodiadas pela Infra S.A., indispensáveis à continuidade do negócio e para o cumprimento de seus objetivos estratégicos.

7.3. **Justificativa econômica da solução:**

7.3.1. A aquisição de uma solução de simulação de ataques cibernéticos é não apenas uma necessidade técnica, mas também uma decisão econômica estratégica. Abaixo, apresentamos os principais aspectos que justificam economicamente essa contratação:

7.3.1.1. Redução de Custos de Incidentes: Investir em uma solução de simulação de ataques cibernéticos permitirá a diminuição significativa dos custos associados a incidentes de segurança. Com a proteção adequada, a Infra S.A. poderá evitar prejuízos financeiros resultantes de vazamentos de dados, interrupções de serviços e multas por não conformidade com regulamentações, como a LGPD.

7.3.1.2. Economia em Suporte e Manutenção: A contratação contempla serviços de atualização, subscrição, manutenção e suporte técnico. Isso significa que a Infra S.A. poderá contar com assistência contínua e atualizações regulares, evitando gastos inesperados com reparos ou atualizações emergenciais, o que proporciona uma gestão financeira mais previsível e controlada.

7.3.1.3. Eficiência Operacional: A solução de simulação de ataques promove a automação e o gerenciamento centralizado, resultando em uma operação mais eficiente. Essa eficiência se traduz em redução de custos operacionais, pois permite que a equipe de TI se concentre em atividades estratégicas, ao invés de gastar tempo e recursos em tarefas manuais ou na resolução de problemas que poderiam ser evitados.

7.3.1.4. Aumento da Produtividade: Com uma infraestrutura de rede segura e disponível, os colaboradores terão acesso rápido e confiável às informações necessárias para o desempenho de suas atividades. Isso não apenas melhora a produtividade, mas também resulta em maior satisfação dos usuários, o que pode levar a um aumento na eficiência geral da organização.

7.3.1.5. Escalabilidade e Adaptabilidade: A solução de simulação de ataques é escalável, permitindo que a Infra S.A. cresça de forma sustentável. Isso significa que novos serviços e funcionalidades podem ser incorporados sem a necessidade de investimentos substanciais adicionais, favorecendo a gestão financeira a longo prazo.

7.3.1.6. Conformidade Regulatória: A adesão a normas e regulamentações, como a LGPD, não só evita multas e penalidades, mas também reforça a imagem da Infra S.A. perante a sociedade e os cidadãos. Uma reputação sólida pode resultar em parcerias e oportunidades de negócios mais vantajosas, ampliando a capacidade de geração de receita.

7.3.1.7. Investimento em Tecnologia de Ponta: A escolha de uma solução avançada de simulação de ataques representa um investimento em inovação e modernização, garantindo que

a Infra S.A. esteja alinhada com as melhores práticas do mercado. Isso não apenas maximiza o retorno sobre o investimento, mas também assegura a competitividade da organização em um cenário de constantes mudanças tecnológicas.

7.3.1.8. Redução de Custos com Incidentes: A validação contínua das ferramentas e a simulação de ataques permitem identificar e corrigir vulnerabilidades antes que sejam exploradas, diminuindo o risco de incidentes dispendiosos. Isso resulta em uma economia significativa ao evitar custos associados a remediação de incidentes e recuperação de dados.

7.3.1.9. Esses aspectos econômicos demonstram que a contratação de uma solução de simulação de ataques cibernéticos é uma decisão estratégica que proporciona não apenas segurança aprimorada, mas também benefícios financeiros substanciais para a Infra S.A.

7.4. **Benefícios a serem esperados:**

7.4.1. Realizar ágil e maciço investimento na tríade de pessoas, processos e tecnologias em governança, gestão e operações de segurança cibernética da empresa, com aporte de pessoal técnico especializado, transferência de conhecimento, metodologia, padronização, estrutura operacional, ferramentas e soluções tecnológicas adequadas;

7.4.2. Prover meios adequados e especializados, em termos de pessoas, processos e tecnologias, para a gestão, implementação e manutenção eficaz dos controles e salvaguardas de segurança cibernética e prover o apoio à gestão e à governança da segurança da informação, à continuidade de negócios em TIC e à gestão de riscos na SUPTI/DIMEI;

7.4.3. Implantar um centro de controle e operações de segurança cibernética que componha as funções básicas de segurança de identificar, proteger, detectar, responder e recuperar, atuando tanto na segurança defensiva e reativa para monitoramento, detecção e resposta gerenciados a eventos e incidentes de segurança, quanto na segurança ofensiva e proativa para gestão contínua de vulnerabilidades e ameaças e para testes de segurança, prestando apoio direto às diversas áreas da SUPTI na prevenção, investigação, remediação e melhorias de cibersegurança;

7.4.4. Elevar o nível de segurança cibernética na Infra S.A., sua maturidade e melhoria contínua, visando estabelecer o nível adequado de controle sobre a confidencialidade, integridade e disponibilidade dos ativos e serviços de TIC e das informações digitais da estatal

7.4.5. Garantir conformidade e alinhamento com os requisitos de negócio, regulamentos pertinentes, a tolerância a riscos e os recursos da organização, em especial observância à estratégia de segurança cibernética da administração pública;

7.4.6. Obter visibilidade ampla sobre a segurança cibernética, a superfície de ataque e os níveis de risco na Infra S.A., tanto ao nível tático-operacional quanto ao nível estratégico-gerencial;

7.4.7. Contribuir na comunicação, difusão e disseminação da cultura e sensibilização dos conceitos, práticas e controles de segurança cibernética na Infra S.A.

8. PARCELAMENTO

8.1. O não parcelamento do objeto é justificado pela **interdependência e integração necessária entre os serviços que compõem a solução contratada** , conforme descrito a seguir:

8.1.1. **Inter-relação entre os serviços:**

8.1.1.1. A maior parte dos serviços envolvidos é altamente inter-relacionada, de forma que sua execução isolada comprometeria a efetividade e a continuidade das ações de segurança cibernética. Por exemplo, as metodologias, processos e procedimentos definidos nos serviços estratégicos (como planejamento e políticas de segurança) são utilizados como base para os serviços reativos e preventivos, como tratamento e resposta a incidentes e gestão de vulnerabilidades. A fragmentação do objeto dificultaria essa inter-relação e colocaria em risco a coerência operacional.

8.1.2. **Dependência dos resultados entre os serviços:**

8.1.2.1. Os resultados obtidos em diagnósticos, análises, testes, eventos e incidentes realizados nos serviços reativos e preventivos são insumos diretos para a elaboração e atualização do plano de controles e salvaguardas de segurança. Qualquer descompasso entre fornecedores ou equipes responsáveis por serviços separados poderia comprometer a confiabilidade das informações e a eficácia das ações decorrentes.

8.1.3. **Harmonia e complementaridade entre diagnósticos e avaliações:**

8.1.3.1. Os diagnósticos e avaliações realizados na fase de implantação e nos serviços estratégicos, bem como nos serviços de identidade e acesso.

8.2. Os serviços continuados devem tirar proveito da mesma infraestrutura tecnológica e operacional 24 × 7 de alta disponibilidade; e as soluções e ferramentas ofertados devem compor uma arquitetura unificada e harmônica, evitando sobreposições, conflitos e lacunas entre si. Portanto, o não parcelamento destes serviços, além de garantir máxima integração e agilidade na execução dos serviços, reduz significativamente a complexidade técnica e administrativa e pode facilitar uma proposição de serviços e soluções otimizada e favorável à economicidade.

8.3. Contudo, o serviço de Testes de Invasão (Pentest), a serem executados de forma esporádica, são testes de segurança nos quais os avaliadores imitam ataques do mundo real, usando as mesmas ferramentas e técnicas usadas por invasores reais, na tentativa de identificar maneiras de contornar os recursos de segurança de aplicativos, sistemas, redes e processos com o objetivo de revelar vulnerabilidades nos sistemas, ativos, controles e processos. Desta forma, eles põem à prova todos os demais serviços e se prestam como um instrumento para simular ataques reais e auditar, na prática, os controles e posturas de segurança cibernética, tal que, pelo princípio de segregação de funções previsto na norma internacional ABNT NBR ISO/IEC 27002:2022 (5.3.a).

9. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

9.1. Não se verifica contratações correlatas nem interdependentes para a viabilidade e contratação desta demanda conforme justificativa abaixo:

9.1.1. A pretensa contratação de uma solução BAS (Simulação de Brechas e Ataques), é uma medida estratégica para fortalecer a postura de segurança cibernética da organização. Embora a solução possa ser integrada com outras contratações e ou contratos vigentes, ela também oferece valor independente ao fazer as seguintes verificações:

a) Identificar e corrigir vulnerabilidades antes que sejam exploradas por atacantes;

b) Fornecimento de uma avaliação contínua e atualizada da postura de segurança;

c) Complementar com outras soluções de segurança, como gestão de vulnerabilidades e detecção e resposta a incidentes;

d) Operação de forma autônoma, permitindo uma avaliação imparcial e contínua da eficácia das defesas cibernéticas.

9.1.2. Portanto, a pretensa contratação da solução de BAS, não ficará sombreada por outras contratações, e sim, vai oferecer um suporte valioso e complementar às iniciativas de modernização de infraestrutura e contratações em nuvem.

10. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

10.1. A contratação da solução é essencial para a atualização técnica da segurança cibernética da estatal, fortalecendo sua capacidade de defesa contra ameaças sofisticadas e garantindo a resiliência operacional. Os resultados esperados destacam-se pela relevância estratégica e técnica:

10.1.1. **Avaliação abrangente da postura de segurança cibernética:**

10.1.1.1. Compreensão técnica e precisa da eficácia dos controles de segurança: A solução permitirá simulações avançadas que avaliam os controles de segurança em todos os níveis, do perímetro aos ambientes internos, fornecimento de avaliações acionáveis e insights críticos para melhorar continuamente a proteção contra ataques.

10.1.1.2. Identificação de vulnerabilidades e brechas:
Diagnósticos detalhados facilitam a identificação de fraquezas exploráveis, permitindo a priorização de correções e a implementação de medidas defensivas mais robustas.

10.1.2. **Capacitação técnica para gerenciamento contínuo de segurança:**

10.1.2.1. Ferramentas avançadas para análise técnica e validação de segurança: A solução fornecerá aos profissionais de segurança cibernética para identificar, diagnosticar, monitorar e gerenciar riscos de forma integrada, promovendo uma visão técnica holística de recursos de postura de segurança.

10.1.2.2. Automação de processos críticos: Tecnologias automatizadas reduzem a intervenção manual, aumentando a eficiência na detecção, validação e resposta a incidentes cibernéticos, enquanto minimizam erros humanos.

10.1.3. **Validação prática e contínua com simulações avançadas (BAS - Breach and Attack Simulation):**

10.1.3.1. Testes realistas e sonoros de segurança: Por meio de simulações contínuas e automatizadas, a solução validará o estado da segurança cibernética frente a ataques reais, ajustando os controles defensivos para lidar com as mais recentes táticas, técnicas e procedimentos (TTPs) usados por adversários.

10.1.3.2. Avaliação de controles em tempo real: Os testes frequentes garantem que a organização mantenha proteção contra ameaças diante da evolução das ameaças, oferecendo uma janela de exposição a vulnerabilidades.

10.1.4. **Proatividade e antecipação de ameaças emergentes:**

10.1.4.1. Identificação antecipada de ameaças: Através da simulação de cenários baseados em ameaças reais, a solução permite prever pontos potenciais de exploração e implementar controles antes que sejam explorados por atacantes.

10.1.4.2. Adaptação às novas táticas de ataque: A integração de inteligência sobre as estratégias adversárias mais recentes possibilitará ajustes rápidos nas defesas, garantindo resiliência contra ameaças emergentes e persistentes.

10.1.5. **Melhoria contínua da maturidade em segurança cibernética:**

10.1.5.1. Medição técnica da maturidade de segurança: Indicadores objetivos e dados técnicos fornecidos pela solução permitirão acompanhar a evolução da segurança cibernética, garantindo alinhamento às melhores práticas globais, como os frameworks da ISO 27001, NIST CSF e MITRE ATT&CK.

10.1.5.2. Ciclo de aprendizado técnico contínuo: Os resultados obtidos servirão como insumos para revisões estratégicas e técnicas, aprimorando os processos de segurança de forma iterativa.

10.1.6. **Impactos técnicos e estratégicos:**

10.1.6.1. Será uma solução essencial para proteger ativos críticos e garantir a continuidade operacional em um cenário de ameaças cibernéticas cada vez mais sofisticadas. Entre os impactos diretos:

10.1.7. **Redução do tempo de detecção e resposta a incidentes:**

10.1.7.1. A solução permitirá que os momentos de segurança identifiquem, analisem e mitiguem ameaças de forma ágil e precisa, reduzidas o impacto de incidentes potenciais.

10.1.8. **Fortalecimento técnico do perímetro de segurança:**

10.1.8.1. Com validações contínuas, a organização manterá controles defensivos ajustados às ameaças mais recentes, diminuindo a probabilidade de sucesso de ataques direcionados.

10.1.9. **Cultura técnica de segurança baseada em dados:**

10.1.9.1. Decisões estratégicas serão fundamentadas em diagnósticos e simulações técnicas propostas, promovendo uma abordagem proativa e informada.

10.2. A solução a ser contratada desempenhará um papel central na evolução da segurança cibernética da Infra S.A., promovendo uma postura técnica de defesa robusta, proativa e resiliente frente às ameaças modernas. Ela não apenas eleva o nível de proteção, mas também prepara a organização para enfrentar os desafios futuros do ambiente cibernético com maior eficiência e confiança.

11. PROVIDÊNCIAS A SEREM ADOTADAS

11.1. **Infraestrutura tecnológica:**

11.1.1. A maior parte dos serviços é remota, não requerendo infraestrutura tecnológica adicional por parte da Infra S.A.. Para os serviços e recursos executados em ambiente externo, a Infra S.A. dispõe da infraestrutura tecnológica suficiente para comportá-los, como pré-disposição no data center e redes de comunicação e acesso à internet.

11.2. **Infraestrutura elétrica:**

11.2.1. Os serviços e recursos internos não devem requerer necessidade adicional de infraestrutura elétrica que demande adequação no ambiente da estatal.

11.3. **Logística de implantação:**

11.3.1. Será provido pela Infra S.A. o acesso físico às suas dependências aos diretamente envolvidos na prestação dos serviços. Assim como no caso do acesso físico, serão fornecidos o acesso lógico e os respectivos privilégios adequados nos sistemas, aplicações, ferramentas e demais ativos necessários à plena execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução, com o devido controle de acesso.

11.4. **Espaço físico:**

11.4.1. A Infra S.A. deverá disponibilizar espaço físico, caso necessário, adequado para comportar a equipe de profissionais da empresa alocados internamente, de acordo com as necessidades do projeto, seja em caráter eventual ou sob demanda (implantações, avaliações etc.).

11.5. **Mobiliário:**

11.5.1. A Infra S.A. deverá disponibilizar o mobiliário básico de cadeiras, mesas de escritório e armários, caso necessário para comportar a equipe de profissionais da empresa nos serviços executados internamente.

12. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

12.1. Os critérios e práticas de sustentabilidade, deverão estar em conformidade com o Guia de Contratações Públicas Sustentáveis da Infra S.A., acessível em www.infrasa.gov.br/pls/.

13. IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

13.1. Para a aquisição de serviços de controle de ataques cibernéticos e testes para ativos de infraestrutura, é importante considerar os impactos ambientais e as respectivas medidas mitigadoras como informado abaixo:

I - **Impacto:** a operação contínua de equipamentos de segurança cibernética, como servidores, firewall e sistemas de monitoramento, pode resultar em um aumento significativo no consumo de energia elétrica.

II - **Medida mitigadora:** Implementar equipamentos de segurança cibernética que sejam energeticamente eficientes e que possuam certificação como a Energy Star. Além disso, adotar prática de gerenciamento de energia, como o uso de sistemas de resfriamento eficientes e a otimização do uso de energia nos data centers.

14. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

14.1. Considerando as informações deste estudo, a Equipe de Planejamento da Contratação, em

harmonia com o disposto na Instrução Normativa nº 94/2022/SGD/ME, e considerando que os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, conclui pela VIABILIDADE DA CONTRATAÇÃO, tendo por fundamento seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade.

14.2. **Justificativa da solução escolhida:**

14.2.1. A proposta de aquisição de uma solução abrangente para segurança, infraestrutura e disponibilidade de dados para o ambiente de datacenter e usuários corporativos é fundamentada na necessidade de garantir um funcionamento robusto, seguro e eficiente das operações da empresa. A seguir, serão detalhados os benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade:

14.2.1.1. Eficácia: a eficácia da solução se refere à capacidade de atender aos objetivos estratégicos da empresa, garantindo a proteção dos dados e a continuidade das operações. Os principais benefícios incluem:

a) Proteção de dados sensíveis: a implementação de soluções de segurança, como firewalls, sistemas de detecção de intrusões e criptografia, minimizará o risco de vazamento de informações confidenciais, assegurando a conformidade com normas regulatórias;

b) Redução de downtime: a infraestrutura projetada para alta disponibilidade garantirá que os serviços estejam sempre acessíveis, evitando perdas financeiras e danos à reputação da Infra S.A.

14.2.1.2. Eficiência: a eficiência está relacionada à otimização dos recursos disponíveis. A solução proposta proporciona:

a) Centralização da gestão: com uma infraestrutura integrada, a gestão de dados e segurança será centralizada, reduzindo o tempo e o esforço necessários para a administração dos sistemas;

b) Automatização de processos: a adoção de tecnologias de automação permitirá a execução de tarefas repetitivas, liberando a equipe de TI para se concentrar em iniciativas estratégicas, melhorando a produtividade geral.

14.2.1.3. Efetividade: a efetividade diz respeito à capacidade de gerar resultados positivos e sustentáveis para a organização. Os impactos incluem:

a) Melhoria na resposta a incidentes: com suporte contínuo e manutenção preventiva, a Infra S.A. estará melhor equipada para responder rapidamente a incidentes de segurança, minimizando os impactos;

b) Capacitação da equipe: o suporte técnico e a formação oferecidos como parte da solução garantirão que a equipe de TI esteja sempre atualizada em relação às melhores práticas de segurança e gestão de dados.

14.2.1.4. Economicidade: a economicidade da solução refere-se à maximização do valor investido. Os benefícios incluem:

a) Redução de custos operacionais: a eficiência na gestão e a diminuição de incidentes de segurança resultarão em menor necessidade de investimentos adicionais em correção de falhas e recuperação de dados;

b) Investimento sustentável: a escolha de uma solução com suporte e manutenção garantidos assegura que o investimento inicial gere retorno a longo prazo, evitando gastos com soluções pontuais e não integradas.

14.3. A contratação de solução para validação de segurança contínua com serviços gerenciados de segurança cibernética (Managed Security Services - MSS) é essencial para a proteção e continuidade das operações da empresa. Com um enfoque em eficácia, eficiência, efetividade e economicidade, a implementação dessa proposta não apenas atenderá às demandas atuais, mas também preparará a organização para os desafios futuros, contribuindo para um ambiente corporativo seguro e produtivo.

14.4. **Necessidade de classificação como sigiloso ou não (artigo 23 da Lei nº 12.527/2011):**

14.4.1. O valor estimado da contratação será **sigiloso**, com base na:

14.4.1.1. Lei nº 13.303/2016:

> Art. 34. O valor estimado do contrato a ser celebrado pela empresa pública ou pela sociedade de economia mista **será sigiloso**, facultando-se à contratante, mediante justificação na fase de preparação prevista no inciso I do art. 51 desta Lei, conferir publicidade ao valor estimado do objeto da licitação, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas.

14.4.1.2. Regulamento Interno de Licitações e Contratos - RILC

> Art.30 § 4º O valor estimado será sigiloso, nos termos do artigo 34 da Lei nº 13.303/16, salvo na hipótese de julgamento por maior desconto, ou justificada a sua publicidade no Termo de Referência ou Projeto Básico.

14.5. A implementação de um orçamento sigiloso para a contratação da pretensa solução é uma medida para proteger os interesses da Infra S.A., garantir a competitividade no mercado e assegurar a integridade e continuidade dos serviços prestados. Essa abordagem alinha-se com as melhores práticas de gestão e segurança, assegurando que a Infra S.A. possa operar de maneira eficiente e responsável em um ambiente cada vez mais desafiador.

15. ASSINATURAS

15.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 360 (9122075), de 29 de novembro de 2024, a qual aprova o presente Estudo Técnico Preliminar da Contratação.

15.2. Conforme o § 2º do Art. 11 da Instrução Normativa 94/2022/SGD/ME, de 23 de dezembro de 2022, o Estudo Técnico Preliminar será aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE	INTEGRANTE ADMINISTRATIVO
(assinatura eletrônica) **Marco Antonio Góes de Oliveira** Assessor Técnico II Matrícula SIAPE: 0446493	*(assinatura eletrônica)* **Robério Ximenes de Saboia** Gerente de Infraestrutura de Tecnologia da Informação Matrícula SIAPE: 1990222	*(assinatura eletrônica)* **Douglas Facundes Balduino** Assistente Administrativo Matrícula SIAPE :2013246

16. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

16.1. Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições do Regulamento Interno de Licitações e Contratos da Infra S.A.

AUTORIDADE MÁXIMA DA ÁREA
(assinatura eletrônica) **Renato Ricardo Alves** Superintendente de Tecnologia da Informação Matrícula SIAPE: 1478523

Aprovo,

AUTORIDADE COMPETENTE

(assinatura eletrônica)
Marcelo Vinaud Prado
Diretor de Mercado e Inovação

Documento assinado eletronicamente por **Renato Ricardo Alves**, **Superintendente de Tecnologia da Informação**, em 16/12/2024, às 17:48, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **MARCO ANTONIO GOÉS DE OLIVEIRA**, **Integrante Técnico**, em 16/12/2024, às 17:49, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Robério Ximenes de Saboia**, **Integrante Requisitante**, em 16/12/2024, às 17:50, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Marcelo Vinaud Prado**, **Diretor de Mercado e Inovação**, em 16/12/2024, às 18:00, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

Documento assinado eletronicamente por **Douglas Facundes Balduino**, **Assistente Administrativo**, em 17/12/2024, às 09:42, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **9164688** e o código CRC **1A1B2B4C**.

Referência: Processo nº 50050.008119/2024-99 SEI nº 9164688

SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5. Bairro Asa Sul, - Bairro Asa Sul
Brasília/DF, CEP 70.070-010
Telefone: