AGENCIA NACIONAL DE TRANSPORTES TERRESTRES

Estudo Técnico Preliminar 108/2026

1. Informações Básicas

Número do processo: 50500.017761/2026-85

2. Descrição da necessidade

Firewall -

2.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da necessidade que consta no Documento de Formalização de Demanda (SEI nº 46540348), referente à contratação de C por meio de Sistema de Registro de Preços, destinados a atender as necessidades da ANTT.

2.2. O(s) serviço(s) objeto desta contratação são caracterizados como comum(ns) , nos termos do inc. XIII do art. 6º, da Lei nº 14.133, de 1º de abril de 2021, pautando-se na premissa que a contratação se baseia em padrões de desempenho e qualidade objetivamente definidos neste documento e seus apêndices, por meio de especificações reconhecidas e usuais do mercado.

2.3. O prazo de vigência da contratação é de 12 (doze) meses, contados da data de assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.4. O processo se enquadra como contratação de TIC, conforme previsto na IN SGD/ME nº 94/2022, art. 2º, inciso VII que define solução de TIC como o “conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC, de acordo com as premissas definidas” em seu Anexo II, são considerados infraestrutura/recurso de TIC os serviços associados ao conjunto de componentes técnicos, hardware, software, bancos de dados implantados, procedimentos e documentação técnica usados para disponibilizar informações, incluindo serviços de segurança digital (controle lógico e biométrico), certificação digital, operação e suporte técnico.

2.4.1. Os serviços e bens, por se tratarem de Contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos, os serviços associados à solução que possuam natureza continuada, pela sua essencialidade, visam atender às necessidades de forma permanente e contínua, por mais de um exercício financeiro, assegurando o funcionamento das atividades finalísticas da ANTT, de modo que sua interrupção comprometerá a prestação do serviço público da Agência e pelo fato de eventual paralisação das atividades contratadas implicar em prejuízo ao exercício das atividades da Administração e no cumprimento de sua missão institucional, A contratação está submetida à Lei nº 14.133/2021 e à IN SGD/ME nº 94/2022.

2.5. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018 , constituindo-se em serviços auxiliares, instrumentais ou acessórios à área de competência legal da ANTT, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos, compreendendo serviços de tecnologia da informação e prestação de serviços de informação, conforme estabelecido pelo inciso XXIII, art. 1º, da Portaria nº 443, de 27 de dezembro de 2018, os quais são preferencialmente objeto de execução indireta, sendo essenciais para o atendimento das necessidades negociais da ANTT.

2.6. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

2.7. O Modelo de Execução do Contrato, nos termos do art. 18 incisos I a V da Instrução Normativa SGD/ME nº 94/2022, define como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento.

Motivação/Justificativa

2.8. A Agência Nacional de Transportes Terrestres (ANTT), autarquia federal responsável pela regulação e fiscalização dos serviços de transporte terrestre, depende de ambiente tecnológico seguro, estável e disponível para a execução de suas atividades finalísticas e administrativas. Seus sistemas corporativos, bases de dados, serviços digitais e recursos de comunicação constituem ativos estratégicos para o cumprimento de sua missão institucional e para a prestação adequada dos serviços públicos.

2.9. Nesse contexto, a solução de proteção de perímetro de rede desempenha papel essencial na segurança da infraestrutura tecnológica da Agência, sendo responsável pela inspeção do tráfego de dados, controle de acessos, prevenção de intrusões, proteção contra ameaças cibernéticas avançadas e monitoramento contínuo dos ambientes de rede.

2.10. Considerando a evolução constante das ameaças cibernéticas e a crescente dependência dos serviços digitais, torna-se necessária a contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, atualizações e subscrições de segurança, suporte técnico especializado, garantia do fabricante, bem como serviços de instalação, configuração, implantação e demais atividades correlatas necessárias à manutenção e evolução tecnológica do ambiente de segurança da informação da ANTT.

2.11. A necessidade decorre da importância de assegurar a continuidade operacional dos serviços de TIC, preservar a confidencialidade, integridade e disponibilidade das informações institucionais e garantir a proteção dos ativos tecnológicos contra acessos não autorizados, ameaças cibernéticas e incidentes de segurança.

2.12. Adicionalmente, a contratação contribuirá para o fortalecimento da postura de segurança cibernética da Agência, permitindo a manutenção de mecanismos atualizados de defesa, monitoramento e resposta a incidentes, em conformidade com a Lei nº 13.709/2018 (LGPD), com as diretrizes da Administração Pública Federal e com as boas práticas estabelecidas pelas normas ABNT NBR ISO/IEC 27001 e 27002.

2.13. A não realização da contratação poderá comprometer a capacidade de proteção do ambiente tecnológico institucional, elevando a exposição da ANTT a vulnerabilidades, indisponibilidades de serviços, incidentes de segurança da informação, riscos operacionais e impactos à prestação dos serviços públicos.

2.14. Dessa forma, a contratação mostra-se necessária para garantir a continuidade, segurança, disponibilidade e modernização da infraestrutura tecnológica da Agência, alinhando-se ao PDTIC, ao Plano de Contratações Anual e aos objetivos estratégicos institucionais voltados à governança, gestão de riscos e transformação digital.

2.15. No âmbito das boas práticas de governança e segurança da informação, a contratação também está alinhada às recomendações estabelecidas pelas normas da família ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, que estabelecem diretrizes e controles relacionados à gestão da segurança da informação, proteção de redes, controle de acessos, monitoramento, gestão de vulnerabilidades e proteção dos ativos de informação. Tais referências constituem boas práticas para o estabelecimento e aprimoramento dos controles de segurança aplicáveis ao ambiente tecnológico da Agência.

2.16. Outrossim, a solução pretendida contribui para o atendimento às diretrizes de segurança da informação e comunicações da Administração Pública Federal, conforme orientações do Gabinete de Segurança Institucional e da Secretaria de Governo Digital, que preconizam a adoção de mecanismos de proteção de rede, controle de acessos e monitoramento contínuo dos ativos de TIC.

2.17. Destaca-se, ainda, a necessidade de implementação de mecanismos de redundância para o enlace do backbone principal, com vistas a assegurar a alta disponibilidade dos serviços e reduzir riscos de indisponibilidade, em consonância com o princípio da continuidade do serviço público.

2.18. Cumpre destacar que a ausência de contratação das licenças de segurança poderá acarretar a exposição da Agência a vulnerabilidades e a diversos vetores de ataques cibernéticos, comprometendo a disponibilidade, integridade e confidencialidade das informações e serviços de TI, além de potencialmente gerar riscos operacionais, financeiros e reputacionais à Administração Pública.

2.19. Por fim, a contratação visa não apenas a modernização da infraestrutura de segurança da rede da ANTT, mas também o fortalecimento da postura de segurança cibernética institucional, a mitigação de riscos operacionais e o atendimento às exigências legais e normativas vigentes, garantindo maior confiabilidade, disponibilidade e proteção dos ativos de informação da Agência.

2.20. Para atingir as metas alinhadas com o planejamento estratégico institucional e traçadas pelo Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a SUTEC busca elevar o nível de qualidade na entrega dos serviços e garantir a continuidade por meio de novos modelos de contratação.

2.21. Nesse sentido, o Mapa Estratégico da ANTT 2020-2030 estabelece, entre seus objetivos estratégicos, o aprimoramento da disponibilidade, qualidade e integração das informações internas e externas, contribuindo para o alinhamento das ações de Tecnologia da Informação e Comunicação às necessidades institucionais e estratégicas da Agência.

2.22. A presente contratação justifica-se pela necessidade de garantir a continuidade, disponibilidade, integridade e confidencialidade dos serviços de Tecnologia da Informação e Comunicação no âmbito da Administração, tendo em vista o papel crítico desempenhado pela solução de inspeção de pacotes de dados (firewall) na proteção da infraestrutura tecnológica institucional.

2.23. A solução atualmente em uso constitui elemento essencial para a defesa do ambiente computacional, sendo responsável por controlar o tráfego de rede, prevenir acessos não autorizados, mitigar ataques cibernéticos (tais como DDoS, ransomware e intrusões), além de assegurar a proteção de dados e sistemas críticos.

2.24. A descontinuidade dos serviços de suporte técnico, atualização de licenças e evolução tecnológica da solução poderá expor a organização a riscos relevantes, tais como:

I - Indisponibilidade de sistemas essenciais;

II - Vazamento ou comprometimento de dados sensíveis;

III - Ocorrência de incidentes de segurança da informação;

IV - Prejuízos à prestação de serviços públicos; e

V - Responsabilização administrativa em face da legislação vigente.

2.25. Destaca-se, ainda, que o cenário atual de ameaças cibernéticas demanda soluções constantemente atualizadas e integradas, especialmente em ambientes modernos baseados em redes definidas por software (SDN), nos quais há aumento significativo do tráfego interno (leste-oeste), exigindo mecanismos avançados de proteção e monitoramento.

2.26. A contratação proposta visa não apenas a manutenção da solução existente, mas também sua evolução tecnológica, com integração a ambientes mais dinâmicos e automatizados, proporcionando maior visibilidade, controle e capacidade de resposta a incidentes de segurança.

2.27. Adicionalmente, a solução escolhida permite o aproveitamento dos investimentos já realizados, evitando custos adicionais com substituição completa de infraestrutura, redução da curva de aprendizagem da equipe técnica e mitigação de riscos operacionais associados à adoção de novas tecnologias.

2.28. Com vistas ao atendimento das necessidades institucionais e ao alcance dos resultados esperados pelas áreas de negócio, informa-se que o Contrato nº 009/2023 (SEI nº 16887271) teve sua vigência encerrada em 06 de junho de 2026, não sendo passível de prorrogação, pois não comporta nova prorrogação, uma vez que atingiu o prazo máximo de vigência contratual previsto na Cláusula Segunda do Contrato e no art. 57, inciso IV, da Lei nº 8.666/1993, aplicável à utilização de programas de informática, cujo prazo máximo é de 48 (quarenta e oito) meses contados do início da vigência contratual. Dessa forma, torna-se necessária a realização de nova contratação para assegurar a continuidade do atendimento da necessidade institucional. O referido contrato contempla os seguintes itens:

LOTE	ITEM	DESCRIÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR ANUAL (R$)
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	27740	Serviço	2	299.350,19	598.700,38
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	27740	Serviço	2	272.728,73	545.457,46
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	27740	Serviço	1	75.109,68	75.109,68
	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	27740	Serviço	4	158.610,93	634.443,72
	5	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	27740	Serviço	1	195.938,30	195.938,30
	VALOR GLOBAL (12 MESES)						2.049.649,54

Justificativa para o não parcelamento da solução TIC

2.29. Os itens contemplam serviços e soluções relacionados à proteção de perímetro da rede corporativa, ao gerenciamento centralizado da segurança, à proteção contra ataques DDoS, à proteção de ferramentas colaborativas em nuvem e ao acesso remoto seguro, os quais atuam de forma complementar na prevenção, detecção e mitigação de ameaças cibernéticas.

2.30. Embora estruturados em itens distintos em razão das especificidades de cada componente, os itens possuem relação funcional no contexto da solução de segurança adotada pela Agência, compartilhando requisitos de integração, gerenciamento, atualização, suporte técnico e tratamento de incidentes.

2.31. A execução por fornecedores distintos poderá resultar na fragmentação da responsabilidade técnica, na necessidade de atuação coordenada de diferentes prestadores para diagnóstico e resolução de incidentes e em dificuldades na identificação da origem de falhas que envolvam mais de um componente da solução.

2.32. Nesse contexto, a contratação em grupo busca assegurar a interoperabilidade entre os componentes, a compatibilidade das configurações e políticas de segurança e a atuação coordenada nos procedimentos de suporte, atualização e resposta a incidentes, reduzindo os riscos decorrentes da fragmentação da execução contratual.

2.33. A adjudicação conjunta também permite concentrar em uma única contratada a responsabilidade pela prestação dos serviços abrangidos pelo grupo, inclusive quanto ao acionamento e à interlocução com os respectivos fabricantes, quando necessário, evitando a transferência de responsabilidade entre fornecedores diante de ocorrências que envolvam componentes distintos da arquitetura de segurança.

2.34. Dessa forma, o não parcelamento decorre da necessidade de preservar a integração operacional da solução e a adequada gestão dos serviços de segurança, desde que demonstrado, nos estudos que fundamentam a contratação, que a adjudicação conjunta não acarreta restrição indevida à competitividade e que existem fornecedores no mercado com capacidade para atender ao conjunto dos itens, preservando-se a obtenção da proposta mais vantajosa para a Administração.

Da adoção do Sistema de Registro de Preços

2.35. Considerando o disposto no Decreto nº 11.462/2023, a adoção do Sistema de Registro de Preços mostra-se adequada às características da contratação, considerando que os serviços serão demandados de forma gradual, conforme as necessidades da ANTT ao longo da vigência da Ata de Registro de Preços, não havendo necessidade de contratação integral dos quantitativos estimados em um único momento.

2.36. A utilização do SRP permite, assim, compatibilizar as contratações com as necessidades efetivamente verificadas durante a vigência da ata, conferindo maior flexibilidade ao planejamento e evitando a contratação antecipada de quantitativos que ainda não sejam necessários.

Da não divulgação do procedimento de Intenção de Registro de Preços

2.37. Entende-se pela não divulgação de Intenção de Registro de Preços (IRP) para participação de órgãos ou entidades externas, nos termos do art. 9º, § 2º, do Decreto nº 11.462/2023, considerando a especificidade da solução pretendida e a necessidade de preservar o planejamento realizado para atendimento das necessidades da ANTT.

2.38. A contratação contempla serviços e soluções de segurança destinados à proteção do ambiente tecnológico da Agência, abrangendo a renovação de suporte técnico e garantia das soluções existentes, o gerenciamento centralizado da segurança, a proteção contra ataques DDoS, a proteção das ferramentas colaborativas em nuvem e o acesso remoto seguro, e os quantitativos e requisitos técnicos foram definidos considerando as características, a arquitetura e as necessidades específicas do ambiente tecnológico da ANTT.

2.39. A eventual adesão de múltiplos órgãos poderia acarretar aumento da complexidade administrativa, dificultando o controle da execução, o acompanhamento das demandas e a gestão dos quantitativos registrados, além de potencialmente impactar o planejamento originalmente estabelecido para atendimento das necessidades institucionais.

2.40. Além disso, tal ampliação poderia introduzir riscos à eficiência, à governança e à segurança do processo de contratação, especialmente em razão da natureza técnica e integrada da solução pretendida.

2.41. Dessa forma, a não divulgação da IRP mostra-se adequada ao planejamento da contratação, permitindo que a Ata de Registro de Preços seja estruturada e gerenciada de acordo com as necessidades específicas da ANTT e com a capacidade de acompanhamento e gestão da Agência.

Da não utilização da Ata por órgão ou entidade não participante

2.42. Diante do contexto apresentado, não será admitida a adesão de órgãos ou entidades não participantes à Ata de Registro de Preços, uma vez que tal permissão implicaria aumento da complexidade operacional e administrativa,com potenciais impactos na gestão da ata, no controle dos quantitativos e na execução contratual, podendo afetar a eficiência, a previsibilidade e a qualidade do atendimento às unidades demandantes.

2.43. Nesse sentido, a vedação à adesão mostra-se necessária para preservar a aderência ao planejamento institucional, assegurar a adequada execução do objeto, garantindo o atendimento prioritário às demandas da Agência.

3. Área requisitante

Área Requisitante	Responsável
GETIC/SUTEC	Marcos Paulo Milanez Santana

4. Necessidades de Negócio

4.1. A solução apresentada deverá incluir todas as funcionalidades definidas neste Estudo Técnico Preliminar, abrangendo licenças de software, aplicativos e sistemas operacionais.

4.2. As necessidades de negócio, ou requisitos do negócio, são metas ou objetivos estratégicos da organização. Elas explicam os motivos para a implementação de um projeto, os resultados esperados e as métricas para avaliar seu sucesso.

4.3. A presente contratação tem por objetivo garantir a continuidade, disponibilidade, integridade e confidencialidade dos serviços de Tecnologia da Informação e Comunicação (TIC), mediante a manutenção e evolução da solução de inspeção de pacotes de dados (firewall) da rede corporativa.

4.4. Assim, seguem abaixo a descrição das necessidades de negócios que orientarão a análise da solução de Firewall, identificando a alternativa mais adequada para atingir esses objetivos:

a) Prevenir e mitigar ataques cibernéticos (DDoS, ransomware, intrusões);

b) Controlar acessos e tráfego de rede;

c) Proteger ativos de informação críticos;

d) Garantir conformidade com normas de segurança e proteção de dados; e

e) Assegurar a continuidade dos serviços institucionais.

4.5. A não contratação implicará riscos relevantes, tais como:

a) Indisponibilidade de sistemas críticos;

b) Vazamento de dados sensíveis;

c) Comprometimento da integridade da rede; e

d) Responsabilização institucional em face da Lei nº 13.709 de 14 de Agosto de 2018.

4.6. Desta forma, com vistas a manter a continuidade dos serviços da Agência e atender à demanda atual e futura para todos os usuários da ANTT, é necessária a contratação de solução que abranja os softwares e os quantitativos descritos na tabela abaixo:

Grupo	Item	Descrição	Catser	Unidade de Medida	Quantidade
1	1	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT.	27740	Serviços	2
	2	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT .	27740	Serviços	2
	3	Serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT.	27740	Serviços	1
	4	Fornecimento de licenças, suporte técnico e garantia , para solução de proteção contra ataques de serviços DDoS.	27740	Serviços	1

	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration.	27740	Serviços	2000
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access.	27740	Serviços	600

4.7. Segue, o detalhamento dos itens e das respectivas necessidades relacionadas a cada solução:

ID	DESCRIÇÃO	NECESSIDADE
1	Contratação do serviço de suporte e manutenção para solução de NG Firewall	O serviço é necessário para assegurar a disponibilidade dos mecanismos de proteção do perímetro da rede e reduzir os riscos decorrentes de falhas, indisponibilidades ou vulnerabilidades que possam comprometer os serviços de TIC da Agência.
2	Renovação de solução de alta disponibilidade para roteamento e proteção de perímetro de rede lógica do tipo Next Generation Firewall (appliances e funcionalidades agregadas) com serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 12 (doze) meses.	A solução é necessária para assegurar a continuidade e a disponibilidade dos mecanismos de proteção do perímetro da rede, permitindo o controle e a inspeção do tráfego, aplicação das políticas de segurança, prevenção e mitigação de ameaças e manutenção da disponibilidade dos serviços protegidos. O regime de suporte técnico 24x7 justifica-se pela criticidade da solução para a infraestrutura de TIC da ANTT e pela necessidade de tratamento de incidentes e falhas que possam ocorrer fora do horário comercial.
3	Renovação de solução de Gerenciamento Centralizado para os Itens 1, 2 e 4 do Grupo 1 com serviço de garantia, atualização e suporte técnico em regime 24x7 por 12 (doze) meses.	A manutenção do suporte e das atualizações da solução de gerenciamento é necessária para garantir sua compatibilidade com os componentes de segurança administrados e preservar a capacidade de gestão e monitoramento do ambiente.
4	Renovação de licenças, suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	A manutenção das licenças e dos serviços associados é necessária para assegurar a atualização dos mecanismos de proteção, a disponibilidade dos recursos de mitigação e o suporte técnico especializado para tratamento de eventos de segurança.
5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony e-mail e collaboration por 12 meses.	A solução destina-se à proteção do ambiente de correio eletrônico e colaboração em nuvem contra ameaças cibernéticas direcionadas aos usuários, incluindo, conforme as funcionalidades contratadas, phishing, malware, roubo de credenciais, mensagens maliciosas e demais ameaças relacionadas ao uso de serviços de colaboração em nuvem.
		A solução deverá contribuir para o controle e a proteção dos acessos realizados remotamente, proporcionando

6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access por 12 (doze) meses.	mecanismos de segurança compatíveis com as políticas institucionais e reduzindo os riscos associados ao acesso a recursos corporativos por meio de redes e ambientes externos.

4.7.1. Todas as licenças deverão estar vigentes pelo período de 12 (doze) meses, o suporte técnico deverá ser prestado em regime 24x7, com atendimento em português deverão estar incluídas atualizações, upgrades e correções de segurança e as soluções devem permanecer totalmente compatíveis com o ambiente tecnológico existente;

4.7.2. A manutenção das licenças e dos serviços de suporte técnico é indispensável para assegurar a continuidade operacional, a integridade dos dados institucionais e a proteção contra ameaças cibernéticas, em conformidade com a Lei nº 13.709/2018 e as boas práticas de segurança da informação.

4.7.3. Ademais, determinado serviço a ser adquirido deverá atender a características técnicas estabelecidas pela Administração e, quando for o caso, às condições de manutenção, assistência técnica e garantia oferecidas. É cabível sempre que houver necessidade e conveniência de se estabelecerem critérios uniformes para as contratações realizadas pela Administração.

4.7.4. Benefícios a serem alcançados na contratação para ANTT:

4.7.4.1. Dentre os principais benefícios a serem alcançados com a contratação, destacam-se :

a) assegurar a continuidade da proteção do perímetro da rede lógica da ANTT, mantendo os mecanismos de inspeção, controle e filtragem do tráfego de rede e de prevenção e mitigação de ameaças cibernéticas;

b) garantir a disponibilidade e a continuidade operacional das soluções, mediante a manutenção dos appliances, funcionalidades agregadas, atualizações de assinaturas de proteção, garantia e suporte técnico especializado;

c) assegurar maior disponibilidade e resiliência da infraestrutura de segurança, por meio da manutenção da solução de alta disponibilidade para roteamento e proteção do perímetro da rede lógica;

d) garantir o gerenciamento centralizado das soluções de segurança, proporcionando maior eficiência na administração das políticas, configurações, eventos, alertas e mecanismos de proteção do ambiente tecnológico;

e) aumentar a capacidade de prevenção, detecção e mitigação de ataques cibernéticos, reduzindo a exposição da infraestrutura tecnológica a vulnerabilidades e ameaças que possam comprometer os serviços institucionais;

f) reduzir os riscos de indisponibilidade decorrentes de ataques de negação de serviço distribuído - DDoS, mediante a manutenção de mecanismos especializados de identificação e mitigação desses ataques;

g) fortalecer a proteção do correio eletrônico e das ferramentas colaborativas baseadas no Microsoft Office 365, reduzindo a exposição dos usuários a phishing, malware, roubo de credenciais e demais ameaças direcionadas aos ambientes de colaboração em nuvem;

h) manter as soluções de segurança atualizadas, mediante a renovação de licenças, subscrições, assinaturas de proteção, atualizações e demais recursos necessários à evolução tecnológica das soluções;

i) garantir suporte técnico especializado em regime compatível com a criticidade do ambiente, especialmente para os componentes que demandam atendimento 24x7, possibilitando resposta adequada a falhas, incidentes e eventos de segurança;

j) aumentar a confiabilidade e a disponibilidade dos serviços de TIC, reduzindo os impactos que eventuais falhas ou incidentes de segurança possam causar às atividades administrativas e finalísticas da Agência;

4.7.5. Com vistas a manter as soluções de segurança cibernética em plenas condições de funcionamento, atualizadas e aptas a enfrentar as ameaças existentes e emergentes, o planejamento da contratação prevê, além da renovação das licenças e subscrições, a manutenção dos serviços associados, incluindo suporte técnico especializado, garantia, atualizações de software e assinaturas de proteção, manutenção das funcionalidades de segurança e demais recursos necessários à continuidade operacional das soluções, pelo período de 12 (doze) meses.

4.7.6. Considerando a natureza continuada dos serviços e a necessidade de manutenção permanente das capacidades de segurança da infraestrutura de TIC, a contratação terá vigência inicial de 12 (doze) meses, podendo ser prorrogada sucessivamente, observados os requisitos legais e a demonstração da vantajosidade para a Administração, pelo prazo máximo de 10 (dez) anos, nos termos dos arts. 106 e 107 da Lei nº 14.133/2021.

4.7.7. Dessa forma, a contratação permitirá à ANTT manter sua infraestrutura de segurança cibernética atualizada, suportada e operacional, reduzindo riscos de indisponibilidade e incidentes de segurança e assegurando a continuidade dos serviços tecnológicos essenciais ao cumprimento de sua missão institucional.

4.8. O objeto da contratação também está alinhado a o Plano Estratégico Institucional - PEI (2026-2029), a o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC (2025-2028) da ANTT, conforme demonstrado abaixo:

ALINHAMENTO AO PLANO ESTRATÉGICO ANTT - 2026-2029	
ID	**Objetivos Estratégicos**
OE 16	Oferecer estrutura física e tecnológica adequada.

ALINHAMENTO AO PDTIC - 2025-2028	
ID	**NECESSIDADES**
NC50	Renovação das licenças de Firewall.
NS 009	Gestão de ameaças e vulnerabilidade em Segurança Cibernética.

ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
M.002	Oferecer estrutura física e tecnológica adequada	IADTI	Índice de Atendimento das Demandas Associadas a Projetos Priorizados (25% em 2026)
		ICMI	Índice de Controles e Medidas Implantados (25% em 2026)

5. Necessidades Tecnológicas

Identificação das necessidades tecnológicas

5.1. As necessidades tecnológicas constam listadas no Apêndice "A" (SEI nº 46545213), deste documento.

5.2. A contratação tem por finalidade atender às necessidades tecnológicas da ANTT relacionadas à proteção, disponibilidade, continuidade e segurança de sua infraestrutura de Tecnologia da Informação e Comunicação -TIC, mediante a manutenção e atualização das soluções atualmente utilizadas e a disponibilização dos recursos necessários à proteção dos diferentes ambientes tecnológicos da Agência.

5.3. Considerando a crescente evolução das ameaças cibernéticas, a necessidade de preservação da disponibilidade dos serviços digitais e a importância da proteção das informações institucionais, torna-se imprescindível garantir:

a) Proteção do perímetro da rede lógica: manter solução capaz de realizar o controle, inspeção e filtragem do tráfego de rede, aplicação de políticas de segurança, prevenção de acessos não autorizados e identificação e mitigação de ameaças cibernéticas;

b) Alta disponibilidade da infraestrutura de segurança: manter os mecanismos de alta disponibilidade associados aos appliances de proteção de perímetro e roteamento, reduzindo pontos únicos de falha e assegurando a continuidade dos serviços protegidos;

c) Suporte e manutenção especializada: assegurar serviços de suporte técnico e manutenção necessários à resolução de incidentes, falhas e problemas relacionados às soluções de segurança, inclusive em regime 24x7 para os componentes de maior criticidade;

d) Atualização das funcionalidades de segurança: manter atualizados os softwares, assinaturas, bases de inteligência, mecanismos de proteção e demais componentes necessários ao funcionamento adequado das soluções e à resposta a novas ameaças cibernéticas;

e) Gerenciamento centralizado: dispor de solução capaz de proporcionar a administração centralizada dos componentes de segurança, permitindo o gerenciamento de políticas, configurações, eventos, alertas e demais recursos de proteção do ambiente tecnológico;

f) Proteção contra ataques DDoS: manter capacidade de identificação e mitigação de ataques de Distributed Denial of Service - DDoS, de modo a reduzir riscos de indisponibilidade dos sistemas, aplicações e serviços institucionais;

g) Proteção de correio eletrônico e colaboração em nuvem: manter solução destinada à proteção das ferramentas colaborativas baseadas no Microsoft Office 365, reduzindo a exposição dos usuários e da organização a phishing, malware, roubo de credenciais e outras ameaças direcionadas ao ambiente de colaboração;

h) Acesso remoto seguro: disponibilizar mecanismos de acesso remoto seguro por meio da solução Harmony SASE - Internet Access, permitindo o acesso controlado aos recursos corporativos por usuários autorizados, em conformidade com as políticas de segurança da Agência;

i) Continuidade tecnológica: evitar a interrupção ou degradação dos recursos de segurança atualmente utilizados, assegurando a continuidade dos serviços de TIC dependentes da infraestrutura protegida;

j) Compatibilidade e interoperabilidade: preservar a integração entre os componentes da arquitetura de segurança existente, reduzindo riscos de incompatibilidade e de indisponibilidade decorrentes de alterações não planejadas na infraestrutura tecnológica;

k) Gestão de vulnerabilidades e riscos: manter mecanismos tecnológicos capazes de contribuir para a prevenção, identificação e mitigação de vulnerabilidades e ameaças que possam comprometer os ativos, sistemas, aplicações e informações da ANTT;

l) Proteção dos ativos e informações institucionais: assegurar mecanismos técnicos destinados à proteção dos ativos de TIC e das informações tratadas pela Agência, contribuindo para a preservação de sua confidencialidade, integridade e disponibilidade;

m) Escalabilidade e evolução tecnológica: possibilitar a manutenção e evolução das capacidades de segurança de acordo com o crescimento do ambiente tecnológico, a evolução das necessidades institucionais e o surgimento de novas ameaças cibernéticas; e

n) Sustentação da infraestrutura existente: preservar os investimentos realizados pela ANTT em infraestrutura, configurações, políticas de segurança, integrações e conhecimento técnico, mediante a manutenção dos recursos necessários à operação das soluções atualmente implantadas.

5.4. As necessidades tecnológicas identificadas evidenciam a importância da adoção de solução robusta de segurança da informação, capaz de garantir a proteção do ambiente computacional, a continuidade dos serviços institucionais e a conformidade com a Lei nº 13.709/2018 e demais normativos aplicáveis.

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

Requisitos Legais

6.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 23 dezembro de 2022 (processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC), à Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 (portaria que estabelece modelo de contratação de software e de serviços de computação em nuvem), à Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021 (procedimento administrativo para a realização de pesquisa de preços), à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), ao Decreto nº 11.462, de 31 de março de 2023 (Sistema de registro de preços para a contratação de bens e serviços), à Resolução nº 6.029, de 7 de dezembro de 2023 (aprova a Política de Segurança da Informação - PoSIN da Contratante), a outras legislações, a outras normas e boas práticas aplicáveis.

Requisitos de Manutenção

6.2. Além dos requisitos de negócio e tecnológicos, destaca-se os requisitos que devem ser considerados ao longo do planejamento da contratação, para garantir o cumprimento dos objetivos pretendidos com a contratação, conforme descrito abaixo:

6.2.1. **Suporte técnico especializado:** disponibilização de suporte técnico especializado para diagnóstico, análise e solução de falhas, indisponibilidades, incidentes e demais ocorrências relacionadas às soluções contratadas;

6.2.2. **Atendimento 24x7:** para os itens definidos como críticos, especialmente as soluções de proteção de perímetro, gerenciamento centralizado e demais componentes cuja indisponibilidade possa comprometer a continuidade dos serviços de TIC, o suporte deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, conforme os níveis de serviço estabelecidos no Termo de Referência;

6.2.3. **Manutenção corretiva:** realização das atividades necessárias à correção de falhas de hardware, software, licenciamento, configuração ou funcionamento que comprometam o desempenho ou a disponibilidade das soluções;

6.2.4. **Manutenção preventiva:** realização de procedimentos destinados à identificação antecipada de falhas, degradações, vulnerabilidades ou condições que possam comprometer o funcionamento adequado das soluções;

6.2.5. **Atualizações de segurança:** disponibilização e aplicação, quando tecnicamente necessárias e autorizadas pela ANTT, de atualizações, correções, patches, novas versões, assinaturas de segurança e bases de inteligência necessárias à manutenção da proteção contra ameaças cibernéticas;

6.2.6. **Atualização das assinaturas de proteção:** manutenção das bases de assinaturas e mecanismos de inteligência necessários à identificação e mitigação de ameaças, especialmente para as soluções de proteção de perímetro e demais componentes que utilizem esse mecanismo;

6.2.7. **Manutenção da garantia:** manutenção da cobertura de garantia dos appliances e demais componentes físicos abrangidos pelo contrato, incluindo reparo ou substituição de componentes defeituosos, conforme as condições estabelecidas neste documento;

6.2.8. **Substituição de equipamentos:** quando aplicável, substituição de equipamentos ou componentes que apresentem defeito e não possam ser recuperados em prazo compatível com os níveis de serviço estabelecidos, por componentes de características técnicas iguais ou superiores, sem prejuízo da continuidade dos serviços;

6.2.9. **Preservação das configurações:** as atividades de manutenção deverão preservar, sempre que possível, as configurações, políticas de segurança, regras, integrações e demais parâmetros existentes, evitando alterações que possam comprometer o funcionamento do ambiente;

6.2.10. **Controle das alterações:** qualquer alteração relevante na configuração ou arquitetura das soluções deverá observar os procedimentos de gestão de mudanças definidos pela ANTT, incluindo planejamento, avaliação de impactos, autorização, execução e registro;

6.2.11. **Backup e recuperação das configurações:** deverão ser observados procedimentos adequados para preservação e recuperação das configurações e políticas de segurança, de modo a permitir a restauração do ambiente em caso de falha ou incidente;

6.2.12. **Monitoramento:** os componentes críticos deverão possuir mecanismos de monitoramento que permitam identificar falhas, indisponibilidades, degradação de desempenho e eventos relevantes de segurança;

6.2.13. **Registro de chamados:** as ocorrências deverão ser registradas em sistema ou mecanismo disponibilizado pela Contratada, contendo, no mínimo, data e hora de abertura, descrição do problema, classificação de criticidade, ações realizadas, responsáveis e data e hora da solução;

6.2.14. **Níveis de serviço:** a Contratada deverá cumprir os prazos de atendimento, resposta, diagnóstico e solução estabelecidos no Termo de Referência e no respectivo Acordo de Nível de Serviço - ANS/Instrumento de Medição de Resultados - IMR, quando aplicável;

6.2.15. **Escalonamento de incidentes:** ocorrências de maior criticidade identificadas pela equipe técnica da ANTT deverão possuir mecanismo de escalonamento técnico capaz de envolver profissionais especializados da Contratada e, quando necessário, do fabricante da solução;

6.2.16. **Suporte do fabricante:** quando a solução depender de suporte especializado do fabricante, a Contratada deverá assegurar o acionamento e acompanhamento dos respectivos canais técnicos, sem transferência indevida dessa responsabilidade para a ANTT;

6.2.17. **Manutenção das licenças e subscrições:** deverão permanecer válidas e regulares, durante toda a vigência contratual, as licenças, subscrições, serviços de atualização e demais direitos necessários ao pleno funcionamento das soluções;

6.2.18. **Continuidade dos serviços:** as atividades de manutenção, atualização ou intervenção deverão ser planejadas de forma a minimizar impactos sobre a disponibilidade dos serviços de TIC da ANTT, preferencialmente mediante execução em janelas de manutenção previamente acordadas;

6.2.19. **Comunicação de indisponibilidades:** a Contratada deverá comunicar previamente intervenções programadas que possam causar indisponibilidade ou degradação dos serviços, ressalvadas situações emergenciais;

6.2.20. **Documentação técnica:** as atividades de manutenção que produzam alterações relevantes deverão ser devidamente documentadas, mantendo-se atualizados os registros técnicos da solução;

6.2.21. Transferência de conhecimento/Orientações técnicas: a Contratada deverá fornecer à equipe indicada pela ANTT orientações técnicas sobre as alterações, atualizações, configurações, integrações ou procedimentos que efetivamente realizar no ambiente, de modo a possibilitar sua compreensão, fiscalização e continuidade pela Contratante.

6.3. As licenças de software deverão ser fornecidas de forma eletrônica (digital).

6.4. Deverão ser entregues com todas as informações necessárias à ativação e utilização;

Requisitos de Segurança e Privacidade:

6.4.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da ANTT (Resolução nº 6.029, de 7 de dezembro de 2023), e observar as seguintes diretrizes:

a) Garantir a aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados.

b) Garantir que, em qualquer hipótese, a Administração detenha a tutela sobre os conhecimentos, informações e dados produzidos no âmbito da prestação dos serviços.

c) Vedar o uso, para fins corporativos próprios, dos conhecimentos, informações e dados produzidos no âmbito da prestação dos serviços.

d) Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, passível de testes periódicos, com o objetivo de assegurar a disponibilidade dos dados e serviços em caso de interrupção.

e) Desenvolver e implementar procedimentos de resposta a incidentes relacionados aos serviços prestados.

6.4.2. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras penalidades previstas na legislação vigente, independente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

6.4.3. A CONTRATADA deverá manter sigilo e confidencialidade sobre todas as informações, dados, documentos e conhecimentos a que tiver acesso ou que venha a tomar conhecimento em razão da execução do objeto, não podendo divulgá-los, reproduzi-los, utilizá-los ou disponibilizá-los a terceiros sem prévia e expressa autorização, por escrito, da CONTRATANTE.

6.4.4. O descumprimento desta obrigação caracterizará falha na execução contratual e sujeitará a CONTRATADA às sanções administrativas cabíveis, na forma da Lei nº 14.133/2021 e do contrato, sem prejuízo da obrigação de reparar integralmente os danos e prejuízos causados à CONTRATANTE ou a terceiros.

6.4.5. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela CONTRATANTE não poderá ser utilizada para fins particulares e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da CONTRATANTE ou acessadas a partir dos seus equipamentos poderão ser auditadas.

6.4.6. Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na CONTRATANTE.

6.4.7. No que couber, o “Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade” deverá ser observado (vide Seção 7 do Anexo da IN SGD nº 94, de 2022. Guia disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf).

Requisitos Sociais, Ambientais e Culturais

6.4.8. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

6.4.9. Requisitos Sociais:

6.4.9.1. A contratada deverá observar integralmente a legislação trabalhista, previdenciária e de saúde e segurança do trabalho aplicável aos profissionais envolvidos na execução contratual.

6.4.9.2. A prestação dos serviços deverá contribuir para a proteção dos ativos de informação da ANTT, assegurando a disponibilidade, integridade e confidencialidade das informações institucionais.

6.4.9.3. A contratada deverá adotar práticas de integridade e responsabilidade social compatíveis com os princípios da Administração Pública, vedadas quaisquer formas de discriminação, trabalho infantil ou trabalho análogo à escravidão.

6.4.10. Requisitos Ambientais:

6.4.10.1. As atividades de suporte técnico, reuniões de acompanhamento, e demais interações relacionadas à execução contratual deverão ser realizadas, sempre que possível e tecnicamente viável, por meios eletrônicos ou remotos, de modo a reduzir a utilização de materiais, a necessidade de deslocamentos e os impactos ambientais associados à execução contratual.

6.4.10.2. Na hipótese de substituição de componentes físicos durante a execução dos serviços de suporte técnico e garantia, a Contratada deverá observar, quando aplicável, as disposições legais e regulamentares relacionadas à gestão e destinação ambientalmente adequada de resíduos eletroeletrônicos.

6.4.11. Requisitos Culturais:

6.4.11.1. A documentação técnica, relatórios, bases de conhecimento, registros de atendimento e materiais de capacitação, quando couber, deverão ser disponibilizados em língua portuguesa ou acompanhados de tradução adequada.

6.4.11.2. Os serviços deverão observar a legislação brasileira, os normativos da Administração Pública Federal e as diretrizes de segurança da informação adotadas pela ANTT.

6.4.12. Os requisitos sociais, ambientais e culturais estabelecidos neste item possuem caráter não exaustivo, devendo a Contratada observar, durante toda a vigência contratual, a legislação, os normativos, os regulamentos e as boas práticas aplicáveis ao objeto, ainda que não expressamente mencionados no Termo de Referência.

Requisitos de Metodologia de Trabalho

6.5. A execução dos serviços está condicionada ao recebimento pela Contratada de Ordem de Serviço (OS) emitida pela Contratante.

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

6.7. A Contratada deve fornecer meios para contato e registro de ocorrências para manutenção corretiva da seguinte forma: com funcionamento de 24 horas por dia e 7 dias por semana de maneira eletrônica e 24 horas por dia e 7 dias por semana por via telefônica.

6.8. A execução do serviço dever ser acompanhada pela Contratada, que dará ciência de eventuais acontecimentos à Contratante.

6.8.1. Será realizada Reunião Inicial entre a Contratante e a Contratada após assinatura de contrato e previamente à emissão de Ordem de Serviço. Serão realizadas quantas reuniões forem necessárias para discussão de assuntos referentes a execução do contrato.

6.8.2. O fornecimento dos serviços está condicionado ao recebimento pelo Contratada de Ordem de Serviços (OS) emitida pela Contratante. A OS indicará o tipo de serviços (licenças), a quantidade e a localidade na qual os serviços deverão ser executados.

6.8.3. O andamento do fornecimento dos serviços deve ser acompanhado pela Contratada, que dará ciência de eventuais acontecimentos à Contratante.

6.8.4. A Contratante realizará a gestão e fiscalização do contrato, bem como o aceite/rejeição dos serviços prestados.

Requisitos de Segurança da Informação e Privacidade

6.8.5. A Contratada deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

6.8.5.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD) , quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

6.8.5.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

6.8.5.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

6.8.5.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pela Contratada.

6.8.5.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da Contratada eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

6.8.5.6. É dever da Contratada orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

6.8.5.7. A Contratada deverá exigir de suboperadores o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

6.8.5.8. A Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a Contratada atender prontamente eventuais pedidos de comprovação formulados.

6.8.5.9. A Contratada deverá apresentar, no prazo de até 48 horas à Contratante, prorrogável por igual período justificadamente, quaisquer informações solicitadas acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

6.8.5.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

6.8.5.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

6.8.5.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a Autoridade Nacional de Proteção de Dados - ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

6.8.5.13. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

6.8.5.14. A Contratada será responsável por garantir que as licenças implementadas contemplem medidas de segurança destinadas à proteção contra acessos não autorizados, à proteção de dados sensíveis e à preservação da integridade das informações tratadas. As atualizações, correções, patches, novas versões, assinaturas de segurança e bases de inteligência disponibilizadas pelo fabricante deverão ser previamente alinhadas com a ANTT e aplicadas quando tecnicamente necessárias e autorizadas pela Contratante, observados os procedimentos e as condições estabelecidos no Termo de Referência.

Sustentabilidade

6.8.6. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos previstos no Guia Nacional de Contratações Sustentáveis e o disposto na Instrução Normativa SLTI/MP nº 1 /2010, no que couber durante a execução do objeto contratado.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A presente seção contém o registro do quantitativo estimado de bens e serviços necessários para a composição da solução a ser contratada, de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, metodologias e técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 .

7.2. A estimativa da demanda para a contratação de empresa especializada no fornecimento de licenças, subscrições, suporte técnico, garantia, atualizações e serviços associados a soluções de segurança cibernética para atendimento das necessidades da ANTT, incluindo os quantitativos de bens e serviços necessários, encontra-se detalhada na tabela a seguir:

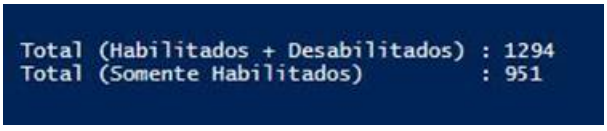
Grupo	Item	Descrição	Unidade de Medida	CATSER	Quantidade
	1	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT.	Serviços	27740	2
	2	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT.	Serviços	27740	2
	3	Serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT.	Serviços	27740	1

1	4	Fornecimento de licenças, suporte técnico e garantia, para solução de proteção contra ataques de serviços DDoS.	Serviços	27740	1
	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration.	Serviços	27740	2.000
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access.	Serviços	27740	600

7.3. Os quantitativos foram estimados com base nas necessidades atuais e projetadas da ANTT, considerando o dimensionamento do ambiente tecnológico institucional, a quantidade de ativos e usuários abrangidos pelas soluções de segurança, os recursos atualmente utilizados e a necessidade de assegurar a continuidade operacional, a evolução tecnológica e a ampliação dos mecanismos de proteção da infraestrutura de TIC da Agência.

7.4. A definição dos quantitativos também considerou a necessidade de manutenção dos recursos atualmente contratados, bem como a ampliação da cobertura de segurança para ambientes, serviços e usuários que demandam proteção adicional, de forma a assegurar atendimento adequado às necessidades institucionais e evitar a existência de ativos ou usuários sem os mecanismos de proteção compatíveis com os riscos aos quais estão expostos:

ITENS	MANIFESTAÇÃO
1 e 2 Renovação de suporte técnico, garantia e atualizações das soluções Check Point SandBlast	A definição dos quantitativos dos itens 1 e 2 foi realizada com base na infraestrutura de segurança atualmente em operação na ANTT e nos equipamentos Check Point instalados e utilizados nos ambientes corporativos da Agência. A presente contratação contempla a renovação dos serviços necessários à continuidade operacional das soluções existentes, incluindo suporte técnico especializado, atualizações de software, garantia do fabricante e manutenção do direito de utilização das funcionalidades contratadas. Os quantitativos correspondem à quantidade de equipamentos atualmente em utilização pela ANTT e refletem a necessidade de manutenção da capacidade de proteção já implantada e integrada ao ambiente tecnológico institucional.
3 Security Management Software	A quantidade estimada de 1 (uma) licença para o Security Management Software foi definida com base na arquitetura de segurança atualmente adotada pela ANTT, que utiliza um ambiente centralizado para gerenciamento, monitoramento e administração das políticas de segurança dos equipamentos Check Point instalados na infraestrutura corporativa. O quantitativo mantém-se inalterado em relação à contratação anterior, uma vez que a solução desempenha a função de gerenciamento centralizado de todo o ambiente de segurança, não havendo necessidade técnica de múltiplas instâncias para atendimento da demanda institucional atualmente existente. A manutenção dessa licença é indispensável para garantir a continuidade das atividades de administração, configuração, auditoria, geração de relatórios, gerenciamento de eventos de segurança e aplicação de políticas corporativas, assegurando a operação integrada dos dispositivos de segurança da ANTT.
	O quantitativo estimado para este item foi definido considerando a necessidade de manutenção da solução de proteção contra ataques distribuídos de negação de

4 Solução de proteção contra ataques DDoS	serviço (DDoS) atualmente utilizada pela ANTT para proteção de seus serviços e sistemas disponibilizados à internet. A contratação contempla a continuidade do licenciamento, suporte técnico, garantia e atualizações da solução pelo período de 12 (doze) meses, assegurando a manutenção dos níveis de disponibilidade, desempenho e proteção dos serviços digitais prestados pela Agência.
5 Solução para proteção de ferramentas colaborativas baseadas no Microsoft 365	A estimativa de 2.000 licenças para a solução de proteção de ferramentas colaborativas baseadas no Microsoft 365 (Harmony Email & Collaboration) foi definida com base na quantidade de usuários que utilizam os serviços corporativos de correio eletrônico e colaboração em nuvem disponibilizados pela ANTT, considerando a necessidade de proteção abrangente do ambiente institucional contra ameaças direcionadas aos serviços de comunicação e colaboração eletrônica. A solução tem por finalidade complementar os mecanismos de segurança nativos da plataforma Microsoft 365, agregando funcionalidades avançadas de proteção contra phishing, spear phishing, comprometimento de contas corporativas (Business Email Compromise - BEC), malware, ransomware, ataques de dia zero e demais ameaças avançadas direcionadas aos usuários e aos serviços de comunicação institucional. O quantitativo de 2.000 licenças foi dimensionado com base na quantidade aproximada de licenças Microsoft atualmente disponibilizadas para utilização institucional, estimada em cerca de 2.050 usuários, disponibilizadas por meio da OS 01/2025 (doc. SEI nº 38125771) do CT 40/2025, e conforme informações fornecidas pela área técnica responsável pela administração do ambiente corporativo. Considerando que a solução é licenciada por usuário e possui como objetivo assegurar proteção homogênea ao ambiente colaborativo institucional, adotou-se quantitativo compatível com a base de usuários potencialmente expostos aos riscos de segurança tratados pela solução, garantindo cobertura adequada das contas corporativas utilizadas pela Agência. Por fim, por tratar-se de solução ainda não utilizada pela ANTT e inexistir histórico específico de consumo que permita aferição precisa da demanda, o quantitativo foi definido mediante estimativa técnica fundamentada nas informações institucionais disponíveis durante o planejamento da contratação, observados os princípios da razoabilidade, proporcionalidade, economicidade e continuidade dos serviços de TIC.
	A estimativa de 600 licenças para a solução Harmony SASE Internet Access foi definida em razão da necessidade de modernização dos mecanismos de acesso remoto seguro utilizados pela ANTT, mediante adoção de arquitetura baseada nos princípios de Zero Trust, controle contextual de acesso, validação contínua de identidade, proteção avançada de navegação e aplicação centralizada de políticas de segurança. O dimensionamento do quantitativo foi realizado com base em informações levantadas pela área técnica responsável, extraídas do ambiente corporativo de gerenciamento de identidades da ANTT em 02/10/2026. O levantamento identificou aproximadamente 1.200 usuários habilitados para acesso remoto por VPN, dos quais cerca de 900 usuários encontravam-se ativos no ambiente institucional:  Embora a solução possua como uma de suas finalidades o aprimoramento dos mecanismos de acesso remoto atualmente utilizados, seu escopo é mais amplo que

6 Solução de Acesso Remoto Seguro Harmony SASE Internet Access	o modelo tradicional de VPN, incorporando funcionalidades adicionais de proteção de navegação, inspeção de tráfego, aplicação de políticas baseadas em identidade e contexto, mitigação de ameaças e proteção dos acessos aos recursos corporativos. Nesse contexto, definiu-se o quantitativo de 600 licenças como estimativa técnica compatível com a demanda institucional atual e potencial, correspondente a parcela representativa do universo de usuários habilitados para acesso remoto, contemplando usuários que realizam atividades em regime remoto, híbrido ou em deslocamento, bem como equipes de fiscalização, gestores, equipes técnicas, colaboradores autorizados e demais perfis que necessitem de acesso seguro aos recursos institucionais durante a vigência contratual. Considerando tratar-se de solução ainda não implantada no ambiente institucional e inexistir histórico consolidado de sua utilização, o quantitativo foi definido com base nas informações disponíveis durante o planejamento da contratação e na previsão de utilização dos perfis potencialmente beneficiados pela solução, observados os princípios da razoabilidade, proporcionalidade, economicidade e continuidade dos serviços de TIC. A solução permitirá a implementação de controles avançados de segurança, inspeção de tráfego, segmentação lógica de acessos, proteção contra ameaças cibernéticas, prevenção contra vazamento de informações e aplicação de políticas de acesso aderentes às melhores práticas de segurança da informação, contribuindo para a redução dos riscos associados aos acessos remotos e para o aumento da maturidade de cibersegurança da ANTT.

7.5. Os quantitativos foram dimensionados de acordo com a natureza de cada item e com as necessidades identificadas durante o planejamento da contratação. Para os itens 1 a 4, foram considerados os ativos, instâncias e soluções atualmente em operação na infraestrutura tecnológica da ANTT, de forma a assegurar a continuidade dos serviços mediante a renovação de suporte técnico, garantia, licenças e atualizações necessárias à manutenção do ambiente existente.

7.6. Para os itens 5 e 6, que representam novas capacidades de segurança a serem incorporadas ao ambiente institucional, o dimensionamento considerou o universo potencial de usuários abrangidos, seus perfis de utilização, os riscos de segurança identificados e as informações institucionais disponíveis durante a fase de planejamento da contratação. Em razão da inexistência de histórico consolidado de utilização dessas soluções no ambiente da ANTT, os quantitativos foram definidos mediante estimativas técnicas fundamentadas nos dados disponibilizados pelas áreas técnicas responsáveis, observados os princípios da razoabilidade, proporcionalidade, economicidade e continuidade dos serviços de TIC.

7.7. Para os itens 1 a 4, não são previstas adequações estruturais relevantes no ambiente, por se tratar predominantemente da continuidade de soluções já implantadas. Para os itens 5 e 6, serão realizadas, quando aplicáveis, atividades de ativação, configuração, integração e testes necessárias à incorporação das novas capacidades ao ambiente institucional, conforme os requisitos técnicos e as condições estabelecidas no Termo de Referência, sem previsão de substituição integral da infraestrutura existente.

7.8. Os quantitativos previstos referem-se ao período de 12 (doze) meses e destinam-se a atender às necessidades de segurança cibernética da ANTT, contemplando a proteção do perímetro da rede, o gerenciamento centralizado das soluções de segurança, a mitigação de ataques DDoS, a proteção do ambiente colaborativo Microsoft 365 e o acesso remoto seguro.

7.9. Adicionalmente, com vistas a manter as soluções em pleno funcionamento, suporte do fabricante e permanentemente atualizadas durante toda a vigência contratual, o escopo da contratação contempla, além do fornecimento de licenças e subscrições, a prestação de serviços associados, incluindo suporte técnico especializado, atualização de versões, disponibilização de assinaturas e bases de inteligência, aplicação de correções de segurança (patches) e demais atividades necessárias à manutenção contínua do ambiente de segurança cibernética da ANTT.

7.10. Esses serviços são essenciais para garantir:

a) continuidade operacional das soluções de segurança e dos serviços de TIC por elas protegidos;

b) atualização permanente dos mecanismos de proteção, incluindo assinaturas, bases de inteligência e correções de segurança;

c) redução da exposição a vulnerabilidades e ameaças cibernéticas;

d) disponibilidade dos serviços críticos, inclusive mediante mecanismos de alta disponibilidade;

e) capacidade de resposta e mitigação de incidentes de segurança, incluindo ataques DDoS;

f) proteção dos serviços de correio eletrônico e colaboração em nuvem utilizados pela Agência;

g) segurança dos acessos remotos aos recursos corporativos;

h) suporte técnico especializado, inclusive em regime 24x7 para os componentes definidos como críticos;

i) preservação da integridade das configurações e políticas de segurança existentes;

j) redução dos riscos associados a falhas, indisponibilidades e descontinuidade de suporte; e

k) manutenção da capacidade de proteção da infraestrutura tecnológica da ANTT durante todo o período contratual.

7.11. Por fim, os quantitativos serão acompanhados durante a execução contratual, de modo a permitir a adequada gestão da demanda, a verificação da aderência das soluções às necessidades institucionais e a adoção de medidas de ajuste ou planejamento futuro, quando necessárias, observados os limites, condições e instrumentos previstos na legislação aplicável e nos respectivos instrumentos contratuais.

8. Levantamento de soluções

8.1. O inc. II do art. 11 da Instrução Normativa SGD/ME n° 94, de 23 de dezembro de 2022 elenca as seguintes orientações a serem seguidas na análise comparativa de soluções:

a) **Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:** foram realizadas pesquisas ao Painel de Preços e contratações similares feitas pela Administração Pública.

b) **As alternativas do mercado:**

Alternativa	Característica	Vantagem principal	Ponto crítico
1. Renovação da solução existente (Continuidade e ampliação da solução existente)	Manutenção do ambiente atual	Continuidade e aproveitamento do investimento	Dependência tecnológica e custo da renovação
2. Substituição por nova plataforma	Implantação de solução equivalente de mercado	Competitividade e atualização tecnológica	Migração, custos e riscos de transição
3. Segurança/Firewall como Serviço	Recursos disponibilizados como serviço	Atualização e previsibilidade	Dependência do prestador e integração
4. Soluções especializadas por camada	Tecnologias distintas para NGFW, DDoS, colaboração e SASE	Especialização e flexibilidade	Maior complexidade de gestão e integração

c) **A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016:** Não se aplica, considerando que a solução demanda tecnologias específicas de segurança da informação não disponíveis no catálogo de software público.

d) **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, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - eARQ Brasil, quando aplicáveis:** Não se aplica, pois não tem relação com o objeto específico da contratação.

e) **As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual:** Não se aplica. Não será necessária adequação do ambiente tecnológico, uma vez que a contratação refere-se à renovação de licenças e suporte de solução já implantada.

f) **Os diferentes modelos de prestação do serviço:** Prestação de serviço continuado de TIC envolvendo renovação de licenciamento, suporte técnico e garantia de solução de segurança (firewall).

g) **Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes:** O modelo escolhido contempla a manutenção das soluções de segurança atualmente utilizadas pela ANTT, por meio da renovação das licenças, suporte técnico, garantia e atualizações dos componentes já implantados, bem como a ampliação das capacidades de segurança cibernética mediante a incorporação das soluções Harmony Email & Collaboration e Harmony SASE Internet Access. Dessa forma, a contratação visa assegurar a continuidade operacional da infraestrutura existente e promover sua evolução tecnológica, sem substituição integral do ambiente atualmente em operação.

h) **a possibilidade de aquisição na forma de bens ou contratação como serviço:** Continuidade do suporte, garantia, licenciamento e atualização de soluções já existentes, cujos serviços e mecanismos de proteção dependem de renovação periódica.

i) **A ampliação ou substituição da solução implantada:** Contratação, por meio do Sistema de Registro de Preços, de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos.

j) **As diferentes métricas de prestação do serviço e de pagamento:** De forma mensal, anual ou correspondente a cada Ordem de Serviço, após a disponibilização e ativação das licenças e subscrições nela previstas conforme definido no instrumento contratual; Condicionado ao atesto da execução dos serviços pelo fiscal do contrato.

9. Análise comparativa de soluções

9.1. A partir do levantamento de mercado e considerando as necessidades de segurança da informação da ANTT, foram identificadas alternativas capazes de atender, em diferentes níveis, aos requisitos de proteção da infraestrutura de rede, continuidade dos serviços, proteção contra ameaças cibernéticas, mitigação de ataques DDoS, segurança das ferramentas colaborativas em nuvem e acesso remoto seguro.

9.2. Para fins de comparação, foram consideradas as seguintes alternativas:

Solução	Nome	Descrição	Avaliação
		A alternativa consiste na manutenção da arquitetura atualmente utilizada pela ANTT, mediante renovação das licenças, subscrições, suporte técnico e garantia dos componentes existentes, além da contratação dos recursos complementares necessários à segurança do ambiente. Apresenta como principal vantagem a **continuidade operacional**, permitindo o	

Solução 1	Renovação da solução existente (Continuidade e ampliação da solução existente)	aproveitamento da infraestrutura, configurações, políticas de segurança, integrações e conhecimentos técnicos já existentes. Além disso, reduz os riscos inerentes à substituição de uma infraestrutura crítica de segurança, evitando, neste momento, custos adicionais relacionados à aquisição de novos appliances, migração de configurações, reestruturação de políticas de segurança, implantação, integração e capacitação da equipe. Entretanto, deverão ser avaliados o ciclo de vida dos equipamentos existentes, a continuidade do suporte pelo fabricante e a relação entre os custos de renovação e os benefícios decorrentes da permanência da solução.	Viável e mais vantajosa. A alternativa atende integralmente às necessidades da ANTT, preserva os investimentos realizados, reduz riscos operacionais e de transição tecnológica, assegura a continuidade dos serviços de segurança cibernética.
Solução 2	Substituição por nova plataforma	A alternativa consiste na substituição integral ou parcial das ferramentas atualmente utilizadas por solução equivalente disponível no mercado. Pode proporcionar atualização tecnológica e ampliar as possibilidades de concorrência. Entretanto, a substituição de uma infraestrutura de segurança já em operação envolve custos diretos e indiretos relacionados à aquisição, implantação, migração, integração, testes, capacitação, adequação dos procedimentos operacionais e eventual indisponibilidade durante a transição. Também seria necessária a reconstrução ou migração das políticas, regras e configurações existentes, além da validação da interoperabilidade da nova solução com os demais componentes do ambiente de TIC.	Não recomendada para a presente contratação. A alternativa demanda substituição da infraestrutura atualmente utilizada, atividades de migração, reconfiguração de políticas de segurança, adequação de integrações, realização de testes, capacitação das equipes e gerenciamento dos riscos inerentes ao processo de transição. Os custos e riscos associados não demonstraram vantajosidade em relação à manutenção da solução atualmente implantada.
Solução 3	Segurança/Firewall como Serviço	Esta alternativa consiste na disponibilização das capacidades de segurança durante determinado período contratual, podendo compreender infraestrutura, licenciamento, atualizações, suporte e serviços associados. O modelo pode reduzir a necessidade de aquisição de ativos e favorecer maior previsibilidade dos custos e atualização tecnológica. Entretanto, demanda avaliação criteriosa de integração com a infraestrutura existente, dependência do prestador, conectividade, níveis de serviço, segurança dos dados e procedimentos de transição ao término do contrato.	Não recomendada para a presente contratação. A alternativa exigiria revisão da arquitetura de segurança atualmente adotada, avaliação de impactos sobre a infraestrutura existente, adequação dos processos de gestão e monitoramento, além de introduzir dependência mais significativa do prestador de serviços. Considerando os investimentos já realizados pela ANTT e os requisitos de continuidade operacional, a

		Para a ANTT, a alternativa também teria que considerar a existência de investimentos já realizados em equipamentos, licenças, configurações e conhecimento operacional.	alternativa não se mostrou mais vantajosa sob a perspectiva técnica, operacional e econômica.
Solução 4	Soluções especializadas por camada	Nesta alternativa seriam contratadas, de forma independente, soluções específicas para firewall, mitigação DDoS, proteção das ferramentas Microsoft 365, acesso remoto seguro e outros mecanismos necessários. A alternativa possibilita selecionar tecnologias especializadas para cada finalidade e reduzir a concentração em um único ecossistema tecnológico. Em contrapartida, tende a elevar a complexidade operacional, uma vez que diferentes plataformas podem demandar múltiplas interfaces de gerenciamento, contratos de suporte distintos, integrações específicas, capacitações técnicas e mecanismos adicionais para correlação e tratamento dos eventos de segurança.	Não recomendada para a presente contratação. A adoção de múltiplas soluções independentes tende a aumentar a complexidade de gerenciamento, integração, sustentação e suporte do ambiente de segurança, demandando maior esforço operacional, maior especialização técnica e ampliação das atividades de administração da solução. Não foram identificados benefícios que justifiquem os custos e riscos adicionais decorrentes dessa abordagem no contexto atual da ANTT.

9.3. A análise comparativa das soluções foi realizada com base em critérios técnicos, operacionais e econômicos, considerando, entre outros aspectos, o grau de aderência ao ambiente tecnológico da ANTT, o aproveitamento da infraestrutura existente, a continuidade operacional dos serviços, os riscos de implantação e migração, a necessidade de investimentos adicionais, a complexidade de gerenciamento, a necessidade de capacitação da equipe, os requisitos de integração com os componentes já existentes, a flexibilidade tecnológica e a relação custo-benefício para a Administração.

9.4. A análise técnica preliminar evidenciou que as quatro alternativas avaliadas possuem potencial para atender, em diferentes níveis, às necessidades da ANTT. Contudo, após a avaliação dos aspectos técnicos, operacionais e econômicos, concluiu-se que a Solução 1 - Renovação e continuidade da solução atualmente implantada apresenta-se como a alternativa mais vantajosa para a Administração.

9.5. Tal conclusão decorre da existência de infraestrutura de segurança já implantada e em operação, da maturidade da equipe técnica na administração da solução, da preservação das integrações e políticas de segurança atualmente utilizadas, da redução dos riscos associados à migração tecnológica e da minimização dos impactos sobre a operação do ambiente de TIC da Agência.

9.6. Adicionalmente, a manutenção da solução existente contribui para a preservação dos investimentos já realizados pela ANTT, evitando custos relacionados à substituição da plataforma tecnológica, à aquisição de novos equipamentos ou licenças, à migração de configurações e políticas de segurança, à realização de testes de interoperabilidade, à capacitação técnica das equipes e à adaptação dos processos operacionais.

9.7. As Soluções 2, 3 e 4 não se mostraram adequadas para atendimento da necessidade da presente contratação. A adoção dessas alternativas exigiria alterações relevantes na arquitetura de segurança atualmente implantada, com necessidade de implantação de novos componentes, migração de configurações e políticas de segurança, realização de integrações adicionais, execução de testes, capacitação das equipes técnicas e adaptação dos processos operacionais e de governança já estabelecidos.

9.8. Além disso, tais alternativas implicariam elevação dos custos diretos e indiretos da contratação, aumento da complexidade de gestão e operação da infraestrutura de segurança e maior exposição a riscos operacionais decorrentes do processo de transição tecnológica, sem a demonstração de ganhos proporcionais capazes de justificar sua adoção no contexto atual da ANTT.

9.9. Dessa forma, considerando os aspectos técnicos, operacionais, econômicos e de gestão de riscos avaliados, conclui-se que a Solução 1 é a única alternativa que atende de forma integral e mais vantajosa aos objetivos de continuidade operacional, segurança, economicidade e eficiência pretendidos pela Administração.

10. Registro de soluções consideradas inviáveis

10.1. Com base no levantamento de mercado e na análise comparativa das alternativas para atendimento da necessidade, foram avaliadas soluções distintas da continuidade do ambiente de segurança atualmente implantado na ANTT.

10.2. Considerando os aspectos técnicos, operacionais, de continuidade, integração e aproveitamento da infraestrutura existente, foram consideradas inviáveis ou inadequadas para a presente contratação, conforme o cenário atual, as alternativas descritas a seguir.

Solução	Nome	Descrição	Motivação
Solução 2	Substituição integral da plataforma de segurança atualmente implantada.	A substituição integral da solução atualmente utilizada por outra plataforma disponível no mercado foi considerada inviável para atendimento da necessidade imediata desta contratação, considerando que a ANTT dispõe de infraestrutura de segurança implantada, configurada, integrada e em operação.	A adoção dessa alternativa implicaria a necessidade de aquisição ou contratação de nova infraestrutura, além da realização de atividades de planejamento de migração, instalação, configuração, integração, reconstrução ou conversão das políticas e regras de segurança, realização de testes, homologação, capacitação da equipe e transição para o novo ambiente. Adicionalmente, a substituição poderia introduzir riscos operacionais relacionados à migração de componentes críticos de segurança e exigir investimentos adicionais para substituição de ativos e licenças ainda integrados à infraestrutura tecnológica da Agência. Dessa forma, diante da necessidade atual de assegurar a continuidade dos mecanismos de proteção já existentes, a substituição integral da plataforma não se mostra, neste momento, a alternativa mais adequada, devendo eventual modernização ou substituição tecnológica ser objeto de planejamento específico, acompanhado das respectivas análises técnica, econômica e de riscos. **Solução considerada inviável para a presente contratação, em razão dos impactos de migração, necessidade de novos investimentos e riscos à continuidade operacional.**
			Embora esse modelo possa oferecer benefícios relacionados à escalabilidade, atualização tecnológica e redução da necessidade de aquisição de determinados ativos, sua adoção integral demandaria alterações relevantes na arquitetura atualmente utilizada pela ANTT, incluindo integrações, revisão de políticas, possíveis mudanças nos fluxos de tráfego e adequações nos procedimentos de administração e monitoramento.

Solução 3	Migração integral para modelo de Segurança como Serviço.	A migração integral para um modelo de segurança disponibilizado como serviço também foi avaliada.	Além disso, para a presente necessidade, sua adoção integral poderia resultar no subaproveitamento dos investimentos já realizados em infraestrutura e soluções de segurança que permanecem em utilização pela Agência. Assim, embora o modelo possa ser considerado em futuras iniciativas de modernização e seja potencialmente aplicável a componentes específicos da segurança, sua adoção integral não se mostra adequada à necessidade imediata de continuidade e sustentação do ambiente atualmente implantado. **Solução considerada inviável como substituição integral do ambiente atual nesta contratação, sem prejuízo de futura avaliação para componentes específicos ou em processos de modernização tecnológica.**
Solução 4	Contratação integralmente fragmentada de soluções especializadas.	Também foi considerada a alternativa de contratação de soluções independentes para cada camada de segurança, com tecnologias e plataformas distintas para firewall, proteção contra DDoS, proteção de ferramentas colaborativas em nuvem, acesso remoto seguro e demais funcionalidades.	Apesar de possibilitar maior flexibilidade na seleção das tecnologias, essa alternativa pode ampliar a complexidade de administração do ambiente, exigindo diferentes consoles de gerenciamento, procedimentos de suporte, integrações, capacitações e mecanismos de correlação dos eventos de segurança. A utilização de diferentes plataformas também demandaria avaliação específica de interoperabilidade com a infraestrutura já existente, podendo aumentar o esforço necessário à operação, administração, monitoramento e tratamento de incidentes. Considerando a necessidade atual de continuidade operacional e integração com o ambiente existente, a fragmentação integral da solução não se mostrou a alternativa mais adequada. **Solução considerada inviável para atendimento integral da presente necessidade, em razão da maior complexidade de integração, gestão, sustentação e operação do ambiente.**

10.3. Após a análise das alternativas, conclui-se que, para o atendimento da necessidade atual, as soluções de substituição integral da plataforma existente, migração integral para Segurança como Serviço e fragmentação integral das diferentes camadas de segurança não se mostram adequadas ao cenário atual da ANTT.

10.4. A continuidade das soluções atualmente implantadas, mediante renovação de suporte técnico, garantia, licenciamento e subscrições, associada à contratação dos recursos complementares necessários, mostra-se tecnicamente mais aderente à necessidade identificada, principalmente por:

a) proporcionar continuidade operacional;

b) preservar a infraestrutura e os investimentos existentes;

c) manter a compatibilidade e interoperabilidade do ambiente;

d) reduzir impactos e riscos de migração;

e) preservar políticas e configurações de segurança em utilização;

f) reduzir a necessidade de reconfiguração e capacitação decorrente de mudança de plataforma; e

g) assegurar atualização, suporte e sustentação dos mecanismos de proteção durante a vigência contratual.

11. Análise comparativa de custos (TCO)

11.1. Nos termos do inciso II do art. 11 da Instrução Normativa SGD/ME nº 94/2022, a análise comparativa de soluções deve contemplar aspectos econômicos e qualitativos, considerando os benefícios associados ao alcance dos objetivos da contratação, observando as seguintes dimensões:

a) cálculo dos custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada licença, a exemplo dos valores de aquisição das licenças, garantia técnica estendida e migração; e

b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

11.2. Adicionalmente, foi elaborada memória de cálculo contendo as premissas e referências de preços utilizadas, de modo a assegurar a rastreabilidade e a transparência dos dados empregados na análise, possibilitando a verificação de sua origem.

11.3. A estimativa de custos foi fundamentada em levantamento de mercado, com base em contratações similares realizadas no âmbito da Administração Pública, incluindo consultas ao Portal Nacional de Contratações Públicas do Governo Federal e análise de contratos vigentes de objetos correlatos.

11.4. A análise comparativa de custos considerou exclusivamente a solução técnica e funcionalmente viável identificada neste Estudo Técnico Preliminar, qual seja, a Solução 1 - Renovação da solução existente (Continuidade e ampliação da solução existente) com renovação das licenças e suporte, uma vez que as demais alternativas foram descartadas na etapa de avaliação de viabilidade.

11.5. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

11.5.1. O custo da alternativa em questão foi elaborado considerando as necessidades atuais e futuras da Agência, cujo valor unitário foi obtido considerando o levantamento registrado no Mapa Comparativo de Preços (SEI nº 46579447).

11.5.2. O dimensionamento do serviço a ser contratado considera o atendimento integral da contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos.

11.5.3. Com base nos parâmetros dispostos na Instrução Normativa SEGES/ME Nº 65, DE 7 DE JULHO DE 2021 , foram realizadas pesquisas ano PNCP, Contratações Públicas mediante consulta ao sítios eletronicos. Do resultado proveniente da consulta, utilizando o código CATSER, 27740 foram localizados 11 Pregões Eletrônicos (SEI nº 41848650), dos quais, apenas 03 (três) pregões apresentaram similaridades ao objeto da contratação pretendida. As informações seguem descritas no quadro abaixo:

Painel de Preços/Comprasnet - Análise/PNCP				
PREGÃO	**ÓRGÃO**	**UASG**	**Objeto**	**ANÁLISE**
			Contratação de atualização tecnológica da atual solução de proteção de rede (firewalls), incluindo hardware e software, bem como licenças, garantia de	Contratação de renovação de licenças envolvendo todos os equipamentos do ambiente de TIC do órgão. Objeto similar, porém não é possível separar os

PE 90.070/2025	Banco Central do Brasil	179087	hardware e software por 48 (quarenta e oito) meses, baseada em tecnologia Check Point, além dos serviços de instalação e repasse de conhecimento.	valores individuais. Além disso, o prazo do contrato é de 48 meses. Dessa forma, não foi possível a utilização do preço como referência.
PE 90001/2025	PROADI – UFMS	154054	ARP 014/2025 – Contratação de solução de segurança de firewall de rede (Next Generation Firewall – NGFW) em cluster. As aquisições contemplam hardware, software de gerenciamento, licenciamento, implantação, configuração, treinamento e atualizações para garantir a Segurança da Informação no ambiente da UFMS.	Contratação de solução de segurança de firewall de rede (Next Generation Firewall - NGFW) em cluster. Não foi possível a utilização do preço como referência.
PE 05/2025	Centro Universitário Municipal de Franca /SP	1074013	Contratação de solução integrada de segurança de rede, composta por equipamento de alto desempenho (Firewall de próxima geração – NGFW) e licenciamento de software por 12 meses.	Contratação de solução integrada de segurança de rede, composta por equipamento de alto desempenho (Firewall de próxima geração - NGFW) e licenciamento de software por 12 meses. Dessa forma, não há como equiparar os valores das licenças e garantias. Os demais itens são de licenças de soluções diferentes ao objeto a ser contratado. Dessa forma, não foi possível a utilização do preço como referência.
PE 006/2025	Fundação Indaiatubana de Educação e Cultura - FIEC	954 - FIEC Indaiatuba	Contratação de empresa(s) para o fornecimento de computadores, equipamentos de rede, segurança, projetores e outras componentes de hardware.	Aquisição de equipamentos e insumos de informática (computadores, workstations, notebooks, access points, servidores, projetores, impressora, SSDs), redes (switches, firewalls, APs) e segurança patrimonial (DVRs, baluns, HDs e câmeras) para modernização e ampliação dos laboratórios escolares, salas de aula e infraestrutura de TI da FIEC com o objetivo de garantir que a tecnologia disponível atenda às demandas pedagógicas, com foco no desempenho, confiabilidade e eficiência energética, conforme Estudo Técnico Preliminar e requisição. Não foi possível a utilização do preço como referência.

Edital nº 90087 /2025	MRJ-PREFEITURA MUNICIPAL DO RIO DE JANEIRO	986001	Contratação de subscrição de licenças de Jira Software Cloud Premium, Jira Service Management Premium, Confluence Premium e plugins extensores de funcionalidades: BigPicture, eazyBI, Jira WorkFlow ToolBox e Timesheet, com suporte técnico, pelo perído de 12 (doze) meses.	Não há como equiparar os valores do objeto. São soluções diferentes ao objeto a ser contratado. Dessa forma, não foi possível a utilização do preço como referência para compor o Mapa de preços.
Edital nº 005/2026	EMPRESA MATO-GROSSENSE DE TECNOLOGIA DA INFORMAÇÃO	202	Contratação de empresa especializada no fornecimento de Licenças de Solução de Firewall de Próxima Geração, incluindo suporte técnico e prestação de serviços especializados.	Não há como equiparar os valores do objeto. São soluções diferentes ao objeto a ser contratado. Dessa forma, não foi possível a utilização do preço como referência para compor o Mapa de preços.
PREGÃO ELETRÔNICO Nº 90020/2025-000 SRP	TRIBUNAL DE JUSTICA DO ESTADO DE MATO GROSSO	925007	Contratação de Solução Integrada de Firewall Checkpoint, por meio de Pregão Eletrônico via Sistema de Registro de Preços para aquisição de equipamentos e licenças com suporte técnico, treinamento, e garantia da fabricante, incluindo equipamentos, softwares, licenciamentos, implantação, horas de consultoria técnica, contemplando, inclusive, os equipamentos e softwares legados.	Objeto similar ao contratado: foram identificados dois itens no levantamento realizado: itens 16 e 19 que foram utilizados como referência para fins de equiparação dos valores relativos às licenças e respectivas garantias, considerando a similaridade entre as soluções e os componentes envolvidos. Dessa forma, foi possível a utilização dos preços como referência.
Edital nº 90013 /2025	TRIBUNAL REGIONAL FEDERAL DA 4A. REGIÃO/RS	90030	Contratação de renovação de garantia, manutenção, suporte, licenças e assinaturas de equipamentos firewall CheckPoint, bom como de atualização tecnológica de hardware e de banco de horas para transferência de tecnológica pelo período de 60 (sessenta) meses.	Objeto similar ao contratado: foi identificado um item similar no levantamento realizado: o item 2, que foi utilizado como referência para fins de equiparação dos valores relativos às licenças e respectivas garantias, considerando a similaridade entre as soluções e os componentes envolvidos.
Termo de Contrato n.º 255 /2025/PGE-DETRAN-RO	GOVERNO DO ESTADO DE RONDÔNIA Procuradoria Geral do Estado - PGE Detran/RO	926002	Aquisição de Licenças de Software de Apoio Técnico da CTI - Checkpoint, para atendimento às necessidades técnico-administrativas deste DETRAN/RO, conforme especificações estabelecidas no Termo de Referência (0058419803).	Objeto similar ao contratado: foi identificado, no levantamento realizado, que o item 2, pode ser utilizado para fins de equiparação dos valores relativos às licenças e respectivas garantias, considerando a similaridade entre as soluções e os componentes envolvidos.

PREGÃO ELETRÔNICO Nº 90087/2025-000	PREFEITURA MUNICIPAL DO RIO DE JANEIRO - RJ	986001	Subscrição de licenças de Jira Software Cloud Premium, Jira Service Management Premium, Confluence Premium e plugins extensores de funcionalidades: BigPicture, eazyBI, Jira WorkFlow ToolBox e Timesheet, com Suporte Técnico, pelo período de 12 (doze) meses, conforme especificações deste Termo de Referência.	Objeto similar ao contratado: Não foi identificado, no levantamento realizado, nenhum item, para ser utilizado como referência para composição do preço.
Pregão Eletrônico nº 005 /2026/MTI	EMPRESA MATO-GROSSENSE DE TECNOLOGIA DA INFORMAÇÃO	N/H	Contratação de empresa especializada no fornecimento de Licenças de Solução de Firewall de Próxima Geração, incluindo suporte técnico e prestação de serviços especializados, conforme condições, quantidades e exigências estabelecidas neste documento.	Objeto similar ao contratado: Não foi identificado, no levantamento realizado,nenhum item, para ser utilizado como referência para composição do preço.

11.5.4. Os valores encontrados nas pesquisas realizadas não foram aproveitados, pois o objeto e as especificações não são similares ao pretendido pela Agência. Já os valores obtidos de Contratos Similares com a Administração Pública (SEI nº 41848650), para a devida composição do Mapa Comparativo de Preços (SEI nº 46579447), em observância aos princípios da razoabilidade e economicidade.

Grupo	Item	Descrição	Unidde de Medida	Quantidade	A PE Nº 90020/2025 TRIBUNAL DE JUSTICA DO ESTADO DE MATO GROSSO		B Edital nº 90013/2025 TRIBUNAL REGIONAL FEDERAL DA 4A.REGIÃO/RS	
					Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT, pelo período de 12 (doze) meses.	Serviços	2	R$ 431.060,00	R$ 862.120,00		
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT pelo período de 12 (doze) meses.	Serviços	2			R$ 737.493,31	R$ 1.474.986,62
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Sotware da ANTT, pelo período de 12 (doze) meses.	Serviços	1				
	4	Fornecimento de licenças, suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviços	1				
	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration por 12 Meses	Serviços	2000				
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access	Serviços	600	R$ 2.084,48	R$ 1.250.688,00		

REFERÊNCIAS					
C Termo de Contrato n.º 255/2025/PGE-DETRAN-RO		D SCANSEC TECNOLOGIA LTDA		E GLOBAL SEC	
Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)
		R$ 386.550,00	R$ 773.100,00	R$ 405.955,00	R$ 811.910,00
		R$ 399.000,00	R$ 798.000,00	R$ 404.740,00	R$ 809.480,00
		R$ 611.500,00	R$ 611.500,00	R$ 569.395,78	R$ 569.395,78
		R$ 2.490.870,00	R$ 2.490.870,00	R$ 2.345.004,00	R$ 2.345.004,00
R$ 526,30	R$ 1.052.600,00	R$ 1.511,00	R$ 3.022.000,00	R$ 1.611,00	R$ 3.222.000,00
		R$ 1.890,00	R$ 1.134.000,00	R$ 2.150,00	R$ 1.290.000,00

MINUTA

F NTESEC SOLUÇÕES EM LTDA		Valor Médio de Referência	
Vlr. Unit.	Vlr. Total (12 meses)	**Vlr. Unit.**	**Vlr. Total (12 meses)**
R$ 376.233,10	R$ 752.466,20	**R$ 399.949,53**	**R$ 799.899,06**
R$ 374.772,40	R$ 749.544,80	**R$ 479.001,43**	**R$ 958.002,86**
R$ 523.088,35	R$ 523.088,35	**R$ 567.994,71**	**R$ 567.994,71**
R$ 2.097.697,81	R$ 2.097.697,81	**R$ 2.311.190,60**	**R$ 2.311.190,60**
R$ 1.326,59	R$ 2.653.180,00	**R$ 1.243,72**	**R$ 2.487.440,00**
R$ 1.614,63	R$ 968.778,00	**R$ 1.934,78**	**R$ 1.160.868,00**
			R$ 8.285.395,23

11.5.5. Considerou-se para esta contratação o valor estimado como referência de preço, em conformidade com os princípios e diretrizes estabelecidos na LEI Nº 14.133, DE 1º DE ABRIL DE 2021, especialmente quanto à busca pela eficiência, economicidade e melhor relação custo-benefício (§1º do art. 11 e art. 23 da referida Lei), bem como com as orientações da INSTRUÇÃO NORMATIVA SEGES/ME Nº 65, DE 7 DE JULHO DE 2021 , que disciplina procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

11.5.6. Para os itens 3 (Security Management) e 4 (proteção contra DDoS), não foram localizados preços em sistemas oficiais nem contratações similares de outros entes públicos compatíveis com o objeto, conforme consultas ao Painel de Preços e ao PNCP. Por isso, os preços foram obtidos por pesquisa direta com fornecedores, nos termos do art. 5º, inciso IV, da IN SEGES/ME nº 65/2021.

11.5.7. O valor estimado de cada item corresponde à média aritmética dos preços coletados, conforme o art. 6º da IN SEGES/ME nº 65/2021. Os preços obtidos em contratações públicas e junto a fornecedores foram analisados criticamente antes do cálculo, e o detalhamento consta do Mapa Comparativo de Preços SEI nº 46579447.

11.6. Definiu-se pela adjudicação em grupo único, composto por 6 (seis) itens, com critério de julgamento de menor preço global, nos termos do art. 82, § 1º, da Lei nº 14.133/2021. Os componentes integram a mesma arquitetura de segurança do fabricante, com subscrições e suporte registrados sob a mesma conta da ANTT e gerenciamento centralizado. A contratação com fornecedores distintos geraria vigências descasadas, conflito de responsabilidade no diagnóstico de incidentes que envolvam mais de um componente e risco de incompatibilidade de versões entre a gerência e os elementos gerenciados, o que torna tecnicamente inviável a adjudicação por item.

11.7. O agrupamento não restringe a competitividade, pois os itens são comercializados pela mesma rede de parceiros autorizados do fabricante, de modo que o parcelamento não ampliaria a disputa (art. 47, § 1º, III). A pesquisa de mercado confirmou a existência de fornecedores aptos a atender ao conjunto, tendo 3 (três) empresas cotado todos os itens (SEI nº 46171662). A modelagem proporciona, ainda, vantagem econômica, ao concentrar em um único contrato a gestão, a fiscalização e a interlocução com o fabricante.

11.8. Desse modo, tem-se que o valor da contratação para 12 meses totaliza em **R$ 8.285.395,23 (oito milhões, duzentos e oitenta e cinco mil trezentos e noventa e cinco reais e vinte e três centavos):**

Grupo	Item	Descrição	Unidade de Medida	CATSER	Quantidade	Valor Unitário	Valor Total
1	1	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT.	Serviços	27740	2	R$ 399.949,53	R$ 799.899,06
	2	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT.	Serviços	27740	2	R$ 479.001,43	R$ 958.002,86
	3	Serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT.	Serviços	27740	1	R$ 567.994,71	R$ 567.994,71
	4	Fornecimento de licenças, suporte técnico e garantia, para solução de proteção contra ataques de serviços DDoS.	Serviços	27740	1	R$ 2.311.190,60	R$ 2.311.190,60
	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration.	Serviços	27740	2.000	R$ 1.243,72	R$ 2.487.440,00
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access.	Serviços	27740	600	R$ 1.934,78	R$ 1.160.868,00
VALOR TOTAL (12 meses)							**R$ 8.285.395,23**

11.9. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

11.9.8. Para fins de estimativa do Custo Total de Propriedade - TCO da solução, considerou-se a estimativa de 36 (trinta e seis) meses, correspondente a três períodos anuais de contratação dos serviços que compõem a solução. O custo estimado para o primeiro período de 12 (doze) meses corresponde a R$ 8.285.395,23 (oito milhões, duzentos e oitenta e cinco mil trezentos e noventa e cinco reais e vinte e três centavos).

11.10. Para fins exclusivamente de projeção do custo total ao longo do horizonte analisado, os valores dos dois períodos subsequentes foram estimados utilizando-se como premissa a aplicação da variação acumulada em 12 meses do Índice de Custos de Tecnologia da Informação (ICTI), calculado pelo Ipea, que correspondia a 3,91% em julho de 2026, última informação disponível à época da elaboração deste estudo.

11.11. Ressalta-se que a utilização desse percentual possui caráter meramente estimativo e foi adotada exclusivamente para subsidiar o cálculo do TCO, não representando previsão dos índices que serão efetivamente apurados nos exercícios futuros, tampouco antecipação de reajuste contratual. Eventuais reajustes observarão o índice efetivamente apurado no período correspondente e as disposições estabelecidas no instrumento contratual.

11.11.1. Assim, considerando a Solução 1, como a única viável para atender às necessidades prementes desta Agência, conforme demonstrado anteriormente, foi alcançado o Custo Total de Propriedade, com base nos dados registrados no Mapa de Comparativo de Preços, o qual segue abaixo:

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)				
Descrição da solução	**Estimativa de TCO**			
	Ano 1	**Ano 2**	**Ano 3**	**Valor Total**
Contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos por registro de preço.	R$ 8.285.395,23	R$ 8.779.204,79	R$ 9.302.445,39	R$ 26.367.045,41

12. Descrição da solução de TIC a ser contratada

12.1. A solução a ser contratada por licitação consiste na contratação de solução de proteção de perímetro, incluindo fornecimento de licenças de software, suporte técnico especializado, atualizações, garantia do fabricante e serviços correlatos por registro de preços, tendo por finalidade assegurar a continuidade operacional, a disponibilidade, a atualização e a sustentação dos mecanismos de proteção da infraestrutura de TIC da ANTT, mantendo os recursos de segurança necessários à inspeção e ao controle do tráfego de rede, à prevenção e detecção de ameaças cibernéticas e à proteção dos ativos tecnológicos da Agência.

12.2. A contratação visa manter os recursos necessários à inspeção e ao controle do tráfego de rede, à prevenção, detecção e resposta a ameaças cibernéticas, bem como à proteção dos ativos tecnológicos e das informações institucionais da Agência.

12.3. A solução deverá contemplar, observadas as condições e funcionalidades previstas nesta contratação:

a) manutenção do suporte técnico especializado;

b) manutenção da garantia dos appliances;

c) disponibilização de atualizações de software, firmware e assinaturas de segurança;

d) acesso às correções, patches e atualizações necessárias à adequada operação da solução;

e) suporte à resolução de incidentes, falhas e problemas técnicos;

f) manutenção da capacidade de proteção contra ameaças cibernéticas conhecidas e emergentes;

g) preservação da compatibilidade com a infraestrutura tecnológica existente; e

h) continuidade da operação da solução sem necessidade de substituição da infraestrutura atualmente instalada.

i) incorporação de novas capacidades de proteção do ambiente de colaboração Microsoft 365 e de acesso remoto seguro.

12.4. Adicionalmente, a contratação contempla a continuidade das capacidades de segurança atualmente utilizadas pela ANTT e a incorporação de novas capacidades de proteção voltadas à segurança do ambiente Microsoft 365 e dos acessos remotos, ampliando o nível de proteção da infraestrutura tecnológica e dos serviços digitais da Agência.

12.5. A solução será utilizada para manter os mecanismos de controle, inspeção e proteção do tráfego de rede, contribuindo para a mitigação de riscos relacionados a acessos indevidos, exploração de vulnerabilidades, códigos maliciosos e demais ameaças à segurança da informação.

12.6. A contratação busca, ainda, preservar os investimentos já realizados pela ANTT, evitando os custos e impactos operacionais decorrentes da substituição imediata dos equipamentos e da implantação de uma nova plataforma de segurança.

12.7. A análise técnica realizada demonstrou que a continuidade das soluções atualmente implantadas, associada à incorporação de novas capacidades de segurança para proteção do ambiente Microsoft 365 e dos acessos remotos, apresenta-se como a alternativa mais vantajosa para o atendimento da necessidade institucional, considerando aspectos técnicos, operacionais e econômicos. A solução permite preservar as integrações existentes e ampliar o nível de proteção da infraestrutura tecnológica da Agência.

12.8. Conclui-se, portanto, que a Solução 1 apresenta-se como a alternativa mais adequada e vantajosa para atender às demandas atuais da ANTT, garantindo a continuidade dos serviços de segurança cibernética, a proteção da infraestrutura tecnológica e a manutenção dos níveis de disponibilidade requeridos pela Agência.

12.9. O detalhamento técnico da solução de TIC a ser contratada encontra-se no Apêndice “A”, deste Estudo Técnico (SEI nº 46545213).

12.10. Os serviços são caracterizados como de natureza continuada, em razão de sua essencialidade para a manutenção da segurança do ambiente computacional da ANTT e para a continuidade dos serviços institucionais, sendo necessários de forma permanente para garantir a adequada proteção da infraestrutura tecnológica e dos ativos de informação da Agência.

12.11. Além disso, os serviços enquadram-se nos pressupostos do Decreto nº 9.507, de 21 de setembro de 2018, constituindo-se em atividades de suporte à infraestrutura tecnológica da Contratante, passíveis de execução indireta, necessárias ao atendimento das necessidades institucionais e ao cumprimento da missão organizacional da ANTT.

12.12. Não é admitida a subcontratação do objeto contratual. A vedação à subcontratação fundamenta-se na necessidade de preservação da responsabilidade técnica integral da futura contratada pela execução dos serviços, pela manutenção da solução, pelo cumprimento dos níveis mínimos de serviço estabelecidos e pelo adequado funcionamento dos mecanismos de segurança contratados. Considerando a natureza integrada da solução de segurança cibernética, a centralização da execução e da responsabilidade técnica contribui para a efetiva gestão contratual, para a rastreabilidade das ações executadas e para a mitigação de riscos operacionais.

12.13. A adoção de solução tecnológica distinta da atualmente implantada demandaria a realização de estudos adicionais, planejamento especializado, atividades de migração, adequações na infraestrutura tecnológica, reconfiguração das políticas e regras de segurança, integração com os ambientes corporativos existentes, validação de interoperabilidade, testes de homologação e eventual capacitação das equipes responsáveis pela administração e operação da solução.

12.14. Tais atividades poderiam aumentar significativamente os riscos operacionais e de indisponibilidade durante o processo de transição, especialmente em razão da criticidade da solução para a proteção da infraestrutura tecnológica da ANTT, da necessidade de preservação das políticas de segurança vigentes e da manutenção dos níveis de disponibilidade exigidos para os serviços institucionais.

12.15. Além dos aspectos técnicos, a eventual substituição da solução atualmente utilizada acarretaria custos adicionais relacionados à implantação da nova plataforma, migração de configurações, reestruturação de processos de segurança, capacitação técnica das equipes, homologação do novo ambiente e realização de testes operacionais, bem como custos decorrentes dos riscos de interrupção ou degradação dos serviços durante o período de transição.

12.16. Ressalta-se que a opção pela manutenção da solução atualmente implantada não decorre de eventual exclusividade de fabricante ou fornecedor, mas da necessidade de assegurar a continuidade operacional, a estabilidade dos serviços, a proteção do ambiente tecnológico e a preservação dos investimentos já realizados pela Administração. Eventuais soluções alternativas somente poderiam ser consideradas caso demonstrassem capacidade de atender integralmente aos requisitos técnicos, funcionais, de interoperabilidade, desempenho, suporte, segurança, disponibilidade e continuidade estabelecidos pela ANTT.

12.17. Dessa forma, considerando a criticidade da infraestrutura de segurança cibernética da Agência, a necessidade de continuidade dos serviços, os riscos inerentes à substituição da plataforma atualmente utilizada e os custos associados à migração tecnológica, conclui-se que a manutenção da solução existente, mediante a contratação de licenças, subscrições,

suporte técnico especializado, atualizações e garantia do fabricante, mostra-se a alternativa mais vantajosa para o atendimento da necessidade institucional, em observância aos princípios da economicidade, eficiência, competitividade, motivação e seleção da proposta mais vantajosa para a Administração Pública.

13. Estimativa de custo total da contratação

Valor (R$): 8.285.398,72

13.1. O custo total da contratação, considerando a composição de itens da solução escolhida, da planilha de custos e da memória de cálculo elaboradas durante a análise comparativa, é de **R$ 8.285.395,23 (oito milhões, duzentos e oitenta e cinco mil trezentos e noventa e cinco reais e vinte e três centavos)** , para o período de 12 (doze) meses, conforme detalhado na tabela abaixo:

Grupo	Item	Descrição	Unidade de Medida	Quantidade	CATSER	Valor Unitário	Valor Total
1	1	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9700 SAND BLAST Appliance da ANTT.	Serviços	2	27740	R$ 399.949,53	R$ 799.899,06
	2	Serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 9300 SAND BLAST Appliance da ANTT.	Serviços	2	27740	R$ 479.001,43	R$ 958.002,86
	3	Serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT.	Serviços	1	27740	R$ 567.994,71	R$ 567.994,71
	4	Fornecimento de licenças, suporte técnico e garantia, para solução de proteção contra ataques de serviços DDoS.	Serviços	1	27740	R$ 2.311.190,60	R$ 2.311.190,60
	5	Solução para proteção de ferramentas colaborativas baseadas no Office 365 na nuvem, Harmony email collaboration.	Serviços	2000	27740	R$ 1.243,72	R$ 2.487.440,00
	6	Solução de Acesso Remoto Seguro Harmony Sase Internet Access.	Serviços	600	27740	R$ 1.934,78	R$ 1.160.868,00
VALOR TOTAL GLOBAL							**R$ 8.285.395,23**

13.2. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

14. Justificativa técnica da escolha da solução

14.1. Compete à ANTT fomentar, regulamentar e avaliar as ações de informatização, direcionadas à manutenção e ao desenvolvimento do sistema de informações e dos sistemas internos de gestão da Agência. Norteada por esta competência, a ANTT desenvolve, pesquisa e incorpora produtos e serviços de tecnologia da informação que possibilitem a implementação de sistemas e a disseminação de informações.

14.2. Para atingir as metas alinhadas com o planejamento estratégico institucional e traçadas pelo Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a SUTEC busca elevar a qualidade na entrega dos serviços e garantir a continuidade por meio de novos modelos de contratação.

14.3. A Tecnologia da Informação e Comunicação (TIC) desempenha um papel crucial na eficiência operacional e na entrega de serviços de qualidade, aprimorando a comunicação interna e externa. A criação de um ambiente colaborativo é essencial na TIC, com o uso de ferramentas robustas para a gestão e análise de dados, possibilitando a coleta, armazenamento, processamento e difusão de informações, contribuindo para a gestão do conhecimento. As Licenças Firewall ajudam a melhorar a eficiência, a segurança e a colaboração no ambiente de trabalho, resultando em uma capacidade de trabalho significativamente aprimorada, além de agilizar processos e tomadas de decisão.

14.4. A escolha da solução objeto da presente contratação decorre da necessidade de assegurar a continuidade, disponibilidade, integridade e confidencialidade da infraestrutura de Tecnologia da Informação e Comunicação - TIC da Agência Nacional de Transportes Terrestres - ANTT, especialmente dos mecanismos responsáveis pela proteção do perímetro da rede, mitigação de ataques cibernéticos, gerenciamento dos recursos de segurança, proteção dos serviços em nuvem e disponibilização de acesso remoto seguro.

14.5. A solução atualmente implantada encontra-se integrada à infraestrutura tecnológica da ANTT e desempenha função essencial na proteção dos ativos de informação e na continuidade dos serviços institucionais. Sua manutenção permite preservar as configurações, políticas de segurança, regras de acesso, integrações, procedimentos operacionais e conhecimentos técnicos já estabelecidos, reduzindo os riscos associados a alterações estruturais no ambiente.

14.6. A solução escolhida contempla, de forma integrada, os seguintes recursos:

a) suporte e manutenção da solução;

b) solução de alta disponibilidade para roteamento e proteção do perímetro da rede lógica;

c) gerenciamento centralizado dos componentes de segurança;

d) proteção contra ataques de Distributed Denial of Service - DDoS;

e) proteção das ferramentas colaborativas baseadas no Microsoft Office 365, mediante solução Harmony Email & Collaboration; e

f) acesso remoto seguro por meio da solução Harmony SASE - Internet Access.

14.7. A manutenção dessa arquitetura apresenta vantagens técnicas relevantes, uma vez que permite a continuidade dos mecanismos de proteção sem a necessidade de substituição imediata da infraestrutura atualmente operacional.

14.7.1. Compatibilidade com o ambiente tecnológico existente:

14.7.2. A solução proposta apresenta compatibilidade com a infraestrutura tecnológica atualmente utilizada pela ANTT, permitindo a manutenção das integrações, configurações e políticas de segurança existentes.

14.7.3. A adoção de solução tecnológica distinta exigiria avaliação de compatibilidade, desenvolvimento ou adaptação de integrações, migração de regras e políticas, realização de testes, homologação e eventual reconfiguração dos demais componentes do ambiente, aumentando a complexidade e os riscos técnicos da contratação.

14.7.4. A continuidade da solução existente reduz esses riscos e permite que a Administração aproveite os investimentos realizados anteriormente em infraestrutura, configuração e capacitação técnica.

14.8. Continuidade e disponibilidade dos serviços:

14.8.1. As soluções de segurança objeto da contratação possuem caráter crítico para o funcionamento da infraestrutura de TIC da ANTT. Eventual indisponibilidade ou redução de suas funcionalidades poderá comprometer o acesso aos sistemas, aplicações, serviços de rede e recursos corporativos.

14.8.2. A manutenção dos mecanismos de alta disponibilidade, suporte técnico, garantia e atualização das soluções permite reduzir a possibilidade de interrupções e assegurar maior resiliência do ambiente tecnológico.

14.8.3. Particularmente nos componentes críticos, a previsão de suporte técnico em regime 24x7 proporciona maior capacidade de resposta diante de falhas e incidentes que possam ocorrer fora do horário comercial.

14.9. Atualização e evolução dos mecanismos de proteção:

14.9.1. O cenário de ameaças cibernéticas apresenta evolução contínua, com surgimento de novas vulnerabilidades, técnicas de exploração e modalidades de ataques.

14.9.2. Nesse contexto, a simples manutenção dos equipamentos físicos não é suficiente para garantir a efetividade da proteção. É necessária a manutenção das licenças, subscrições, assinaturas de segurança, bases de inteligência, atualizações, correções e novas versões, conforme aplicável a cada solução.

14.9.3. A contratação permitirá que os mecanismos de segurança permaneçam atualizados e aptos a responder às ameaças identificadas durante a vigência contratual.

14.10. Gerenciamento integrado da segurança:

14.10.1. A manutenção da solução de gerenciamento centralizado possibilita a administração integrada dos componentes de segurança, favorecendo a padronização das políticas, o monitoramento de eventos, a identificação de ocorrências e a resposta a incidentes.

14.10.2. Sob o ponto de vista operacional, o gerenciamento centralizado reduz a complexidade administrativa e permite maior eficiência das equipes responsáveis pela segurança da infraestrutura de TIC.

14.11. Proteção contra ataques DDoS:

14.11.1. A manutenção da solução específica de proteção contra ataques DDoS proporciona uma camada adicional de segurança destinada à mitigação de eventos capazes de provocar indisponibilidade de serviços e aplicações.

14.11.2. A continuidade dessa capacidade é tecnicamente relevante em razão da necessidade de assegurar a disponibilidade dos serviços institucionais e reduzir os impactos decorrentes de ataques de negação de serviço.

14.12. Proteção do ambiente de colaboração em nuvem:

14.12.1. A manutenção da solução de proteção do ambiente Microsoft Office 365 contribui para reduzir os riscos associados às ameaças direcionadas aos serviços de correio eletrônico e colaboração utilizados pelos usuários da ANTT.

14.12.2. A solução deverá permanecer atualizada e suportada, permitindo o emprego de mecanismos de proteção compatíveis com a evolução das ameaças direcionadas aos ambientes de colaboração em nuvem.

14.13. Segurança do acesso remoto:

14.13.1. A manutenção da solução de acesso remoto seguro possibilita que usuários autorizados acessem recursos corporativos sob mecanismos de controle e proteção compatíveis com as políticas institucionais de segurança.

14.13.2. Essa capacidade é particularmente relevante diante da necessidade de disponibilização de serviços corporativos para usuários que eventualmente estejam fora da infraestrutura física da Agência.

14.14. Redução dos riscos de migração:

14.14.1. A substituição da arquitetura atualmente implantada por solução de outro fabricante implicaria a execução de atividades de planejamento, implantação, configuração, integração, testes, homologação, migração e capacitação.

14.14.2. Além dos custos diretamente relacionados a essas atividades, haveria aumento do risco operacional durante o período de transição, especialmente em razão da criticidade dos componentes de segurança.

14.14.3. A manutenção da solução existente reduz significativamente esses riscos, permitindo que a Administração concentre os esforços na continuidade e evolução dos serviços, sem necessidade de alteração estrutural imediata da arquitetura de segurança.

14.15. Preservação do conhecimento técnico:

14.15.1. A continuidade da solução também permite o aproveitamento do conhecimento acumulado pelas equipes técnicas da ANTT em relação à administração, operação, configuração, monitoramento e tratamento de incidentes relacionados ao ambiente.

14.15.2. Esse fator contribui para reduzir a curva de aprendizado e os custos de capacitação associados à eventual adoção de tecnologia completamente distinta.

14.16. Diante dos aspectos analisados, conclui-se que a solução proposta apresenta adequação técnica às necessidades da ANTT, especialmente por permitir a continuidade da arquitetura de segurança existente, preservar as integrações e configurações já estabelecidas, manter os mecanismos de proteção atualizados e suportados e reduzir os riscos técnicos e operacionais associados à substituição da infraestrutura atualmente utilizada.

14.17. A escolha da solução não se fundamenta exclusivamente na manutenção da tecnologia existente, mas na avaliação de sua aderência aos requisitos técnicos, de segurança, disponibilidade, interoperabilidade, suporte, continuidade e desempenho necessários ao ambiente da Agência.

14.18. Assim, a solução mostra-se tecnicamente adequada para atender às necessidades identificadas no presente Estudo Técnico Preliminar, proporcionando condições para a manutenção e o aprimoramento da postura de segurança cibernética da ANTT e contribuindo para a continuidade dos serviços de TIC essenciais ao cumprimento de sua missão institucional.

14.19. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

14.19.1. A definição da forma de parcelamento considerou as características dos componentes que integram a solução de segurança cibernética da ANTT, sua compatibilidade com o ambiente tecnológico existente, a necessidade de continuidade dos serviços, os aspectos relacionados ao suporte técnico e à gestão de incidentes, bem como os impactos técnicos, operacionais e econômicos decorrentes da eventual contratação dos itens por fornecedores distintos.

14.19.2. Em atendimento ao disposto na Lei nº 14.133/2021, foi realizada análise quanto à possibilidade de parcelamento do objeto, considerando as características técnicas da solução, a necessidade de compatibilidade entre seus componentes, a responsabilidade técnica pela execução, os impactos na gestão contratual, a continuidade dos serviços de segurança da informação e a busca pela solução mais vantajosa para a Administração.

14.19.3. O objeto da presente contratação contempla a renovação e/ou fornecimento de licenças, subscrições, suporte técnico e garantia relacionados às soluções de segurança cibernética utilizadas pela ANTT, abrangendo, entre outros componentes, appliances Check Point SandBlast, software de gerenciamento de segurança, solução de proteção contra ataques DDoS, proteção de ferramentas colaborativas baseadas em Microsoft 365 e solução de acesso seguro à Internet baseada em arquitetura SASE.

14.19.4. A equipe de planejamento avaliou a possibilidade de contratação dos itens de forma individualizada. Embora os objetos sejam passíveis de descrição e quantificação individual, verificou-se que a fragmentação da contratação em fornecedores distintos poderá aumentar a complexidade operacional, administrativa e técnica da gestão, especialmente em situações que demandem atuação coordenada para identificação, tratamento e resolução de incidentes de segurança.

14.19.5. A análise também considerou que parte significativa dos itens está inserida no mesmo ecossistema tecnológico de segurança da informação, envolvendo licenciamento, atualização, suporte e manutenção de soluções que devem permanecer compatíveis com o ambiente tecnológico existente na ANTT. Nesse contexto, a contratação integrada proporciona maior previsibilidade quanto à continuidade dos serviços, à atualização das soluções e à responsabilização técnica do fornecedor.

14.19.6. A opção pelo agrupamento dos itens deverá, entretanto, estar respaldada pela demonstração de que a modelagem adotada proporciona vantagem econômica e/ou técnica para a Administração, não sendo suficiente, por si só, a alegação de facilidade de gestão contratual.

14.19.7. Assim, a formação do grupo único decorre da avaliação conjunta dos aspectos técnicos, operacionais, de segurança e econômicos identificados no presente Estudo Técnico Preliminar.

14.19.8. A contratação conjunta possibilita a centralização da responsabilidade pela prestação dos serviços, especialmente nos casos de incidentes que possam envolver mais de um componente da solução.

14.19.9. A existência de fornecedores distintos para componentes tecnicamente relacionados poderia resultar em dificuldades para determinar a origem de determinados incidentes, bem como em eventual sobreposição ou lacuna de responsabilidades, aumentando o tempo necessário para diagnóstico e solução.

14.19.10. A contratação por grupo único, portanto, favorece a definição de uma responsabilidade técnica centralizada, simplificando o acompanhamento, a fiscalização, a aplicação dos níveis de serviço e a apuração de eventuais falhas na execução contratual.

14.19.11. Nessa hipótese, recomenda-se a contratação em grupo único, contemplando os itens relacionados às soluções de segurança cibernética objeto deste Estudo Técnico Preliminar, pelos seguintes fundamentos:

a) necessidade de assegurar a compatibilidade e a integração dos componentes da solução;

b) continuidade dos serviços de segurança da informação atualmente utilizados pela ANTT;

c) centralização da responsabilidade técnica e do suporte;

d) redução dos riscos de conflitos de responsabilidade entre fornecedores;

e) simplificação da gestão e fiscalização contratual;

f) redução dos custos administrativos decorrentes da gestão de múltiplos contratos;

g) maior eficiência na gestão de incidentes e na resolução de problemas que envolvam componentes interdependentes; e

h) preservação da disponibilidade, segurança e continuidade dos serviços tecnológicos da Agência.

14.20. Ressalta-se que a análise técnica e a pesquisa de mercado realizadas no âmbito da presente contratação demonstraram a compatibilidade da modelagem adotada com as condições praticadas pelo mercado, bem como a existência de fornecedores com capacidade para atendimento ao conjunto dos itens abrangidos pela solução.

14.21. Dessa forma, conclui-se que a contratação em grupo único constitui a alternativa mais adequada para atendimento da necessidade identificada, por proporcionar integração operacional, centralização da responsabilidade técnica, maior eficiência na gestão dos serviços e adequada relação entre os aspectos técnicos e econômicos da contratação, observados os princípios da eficiência, economicidade, competitividade e seleção da proposta mais vantajosa para a Administração, nos termos da Lei nº 14.133/2021.

15. Justificativa econômica da escolha da solução

15.1. Nos termos do art. 47 da Lei nº 14.133/2021, o parcelamento do objeto deve ser adotado sempre que técnica e economicamente viável, com vistas à ampliação da competitividade e à obtenção da proposta mais vantajosa para a Administração, observando-se os princípios da eficiência, economicidade e competitividade.

15.2. A solução escolhida apresenta-se como a alternativa mais vantajosa sob o aspecto econômico, tendo em vista o aproveitamento dos ativos já existentes, evitando custos elevados com substituição integral da infraestrutura.

15.3. A manutenção e renovação das licenças, subscrições, suporte técnico e garantia permitem preservar os investimentos já realizados em equipamentos, configurações, políticas de segurança, integrações e capacitação técnica, reduzindo a necessidade de novos investimentos para implantação de uma plataforma tecnológica distinta.

15.4. Adicionalmente, reduz o custo total da contratação ao eliminar despesas com aquisição de novos equipamentos, implantação, migração e capacitação da equipe, resultando em menor custo total de propriedade (TCO).

15.5. A opção adotada também contribui para a redução de custos indiretos e riscos financeiros, ao evitar interrupções de serviços e retrabalhos decorrentes da implementação de nova solução.

15.6. A análise econômica deverá considerar, ainda, os valores obtidos na pesquisa de preços e as condições praticadas pelo mercado, de modo a confirmar que os preços da solução pretendida são compatíveis com aqueles praticados para objetos de natureza e características equivalentes.

15.7. Dessa forma, a escolha da solução mostra-se economicamente justificável por possibilitar o aproveitamento dos investimentos já realizados pela ANTT, reduzir custos de transição tecnológica e contribuir para a continuidade dos serviços de segurança da informação, sem prejuízo da necessária comprovação da vantajosidade econômica por meio da pesquisa de preços.

15.8. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

15.9. Em atendimento ao princípio do parcelamento previsto na Lei nº 14.133/2021, foi avaliada a possibilidade de contratação dos itens de forma individualizada, considerando os potenciais efeitos dessa modelagem sobre a competitividade, a economicidade e os custos de gestão contratual.

15.10. Embora os itens possam ser individualmente identificados e quantificados, a contratação em grupo único mostra-se economicamente adequada. Como já mencionado anteriormente,os componentes integram a mesma arquitetura de segurança do fabricante, com subscrições e suporte registrados sob a mesma conta da ANTT e gerenciamento centralizado. A contratação com fornecedores distintos geraria vigências descasadas, conflito de responsabilidade no diagnóstico de incidentes que envolvam mais de um componente e risco de incompatibilidade de versões entre a gerência e os elementos gerenciados, o que torna tecnicamente inviável a adjudicação por item. O agrupamento não restringe a competitividade, pois os itens são comercializados pela mesma rede de parceiros autorizados do fabricante, de modo que o parcelamento não ampliaria a disputa (art. 47, § 1º, III). A pesquisa de mercado confirmou a existência de fornecedores aptos a atender ao conjunto, tendo 3 (três) empresas cotado todos os itens (SEI nº 46171662). A modelagem proporciona, ainda, vantagem econômica, ao concentrar em um único contrato a gestão, a fiscalização e a interlocução com o fabricante.

15.11. Nesse contexto, a contratação em grupo único mostra-se economicamente justificável quando comprovado que o agrupamento proporciona melhor relação custo-benefício do que a contratação individualizada dos itens, sem prejuízo da competitividade do certame.

15.12. Assim, conclui-se que o não parcelamento do objeto encontra fundamento na necessidade de conciliar economicidade, eficiência operacional e adequada gestão contratual.

16. Contratações correlatas/Interdependentes

16.1. Não foram identificadas contratações correlatas e/ou interdependentes necessárias à viabilidade da presente contratação.

16.2. Dessa forma, a contratação pretendida é autônoma e independente quanto ao seu objeto, não dependendo da realização de outras contratações para sua execução e pleno atendimento à necessidade identificada.

17. Benefícios a serem alcançados com a contratação

17.1. A contratação pretendida tem como objetivo assegurar a continuidade, a disponibilidade, a segurança e a adequada operação das soluções de segurança cibernética utilizadas pela ANTT, mediante o fornecimento de licenças, subscrições, suporte técnico, atualizações e garantia, conforme as características e quantitativos definidos neste Estudo Técnico Preliminar.

17.2. Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

a) Continuidade dos serviços de segurança da informação;

b) Manutenção da proteção da infraestrutura tecnológica;

c) Atualização das soluções de segurança;

d) Proteção dos serviços corporativos e ferramentas de colaboração;

e) Segurança no acesso à Internet e aos recursos corporativos; e

f) Eficiência e economicidade na aplicação dos recursos públicos.

17.3. Como resultado global, espera-se manter um ambiente tecnológico mais seguro, disponível, resiliente e protegido contra ameaças cibernéticas, assegurando a continuidade dos serviços de TIC essenciais ao funcionamento da ANTT e proporcionando melhores condições para que as unidades administrativas e técnicas desempenhem suas atividades institucionais.

17.4. A contratação deverá, portanto, contribuir diretamente para a continuidade operacional, proteção dos ativos de informação, redução da exposição a riscos cibernéticos, disponibilidade dos serviços, eficiência operacional e economicidade, observados os níveis de serviço e demais requisitos estabelecidos no instrumento de contratação.

18. Providências a serem Adotadas

18.1. A área requisitante deverá realizar o acompanhamento contínuo da execução contratual, com o objetivo de assegurar a continuidade dos serviços, o cumprimento das obrigações estabelecidas e a manutenção dos níveis de serviço previstos no instrumento de contratação, adotando medidas preventivas para evitar interrupções não programadas.

18.2. A área requisitante deverá manter sob sua gestão e disponibilidade o conhecimento necessário à fiscalização, utilização, administração e continuidade das soluções contratadas, incluindo, no que couber, informações de licenciamento, configurações realizadas no ambiente da ANTT, políticas e integrações implementadas, procedimentos operacionais, registros de suporte e documentação técnica disponibilizada pelo fabricante ou produzida durante a execução contratual, de modo a reduzir riscos de dependência excessiva em relação à Contratada.

18.2.1. A preservação desse conhecimento será assegurada mediante a entrega e atualização da documentação técnica e, quando houver implantação, configuração, integração, atualização ou intervenção relevante no ambiente, por meio de orientações técnicas específicas à equipe indicada pela ANTT, conforme disciplinado no Termo de Referência.

18.3. Todos os eventos relevantes ocorridos durante a execução contratual deverão ser registrados em instrumento ou sistema apropriado, contemplando, conforme aplicável, ocorrências, chamados, incidentes, indisponibilidades, alterações e configurações realizadas, providências adotadas, prazos de atendimento, resultados obtidos e demais informações necessárias à fiscalização, à formação do histórico técnico e à continuidade das soluções.

18.4. Os riscos identificados durante a fase de planejamento estão relacionados no Mapa de Gerenciamento de Riscos (SEI nº 40693569), que deverá ser acompanhado e, quando necessário, atualizado ao longo das fases de contratação e execução, especialmente diante da ocorrência de novos riscos ou de alterações nas condições inicialmente previstas.

18.5. A ANTT irá designar equipe para fiscalização e gestão do contrato nos moldes do Art. 29 da Instrução Normativa SGD /ME nº 94, de 23 de dezembro de 2022 . A Contratada deverá designar preposto para representar a empresa e atuar como principal interlocutor junto a ANTT.

18.6. A comunicação entre a equipe de fiscalização e o preposto deverá observar os canais e procedimentos definidos no Termo de Referência, assegurando rastreabilidade das solicitações, dos atendimentos e das providências adotadas.

18.7. Essas providências têm por finalidade assegurar a adequada governança da contratação, reduzir riscos de descontinuidade, preservar o conhecimento institucional, evitar dependência excessiva do fornecedor e garantir que a ANTT mantenha capacidade de acompanhamento, fiscalização e gestão efetiva dos serviços durante todo o período de execução contratual.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

19.1. Esta equipe de planejamento declara viável esta contratação.

19.1.1. Justificativa da Viabilidade

19.1.2. Com base nos estudos técnicos realizados, no levantamento das necessidades institucionais, na análise das alternativas disponíveis no mercado e na avaliação dos aspectos técnicos, operacionais, econômicos e de segurança da informação, conclui-se pela viabilidade da contratação da solução de Tecnologia da Informação e Comunicação (TIC)

destinada à renovação e/ou fornecimento de licenças, subscrições, suporte técnico, atualizações e garantia das soluções de segurança cibernética utilizadas pela ANTT.

19.1.3. A contratação contempla soluções relacionadas à proteção dos appliances Check Point 9700 e 9300 SandBlast, ao Security Management Software, à proteção contra ataques distribuídos de negação de serviço (DDoS), à proteção de ferramentas colaborativas baseadas em Microsoft 365 – Harmony Email & Collaboration e ao Harmony SASE Internet Access, pelo período de 12 (doze) meses, conforme requisitos, quantitativos e condições estabelecidos neste Estudo Técnico Preliminar.

19.1.4. Para fins de declaração da viabilidade da contratação, foram considerados os resultados alcançados pelo planejamento, abrangendo os aspectos de eficácia, eficiência, efetividade e economicidade, conforme apresentado a seguir.

19.1.5. A solução proposta mostrou-se tecnicamente adequada às necessidades identificadas, considerando:

a) compatibilidade com a infraestrutura tecnológica atualmente utilizada pela ANTT;

b) continuidade dos serviços e funcionalidades de segurança já implantados;

c) aproveitamento dos appliances e demais ativos existentes;

d) manutenção das licenças, subscrições, atualizações e mecanismos de proteção necessários ao funcionamento das soluções;

e) atendimento aos requisitos de segurança da informação identificados no planejamento;

f) capacidade de integração com o ambiente tecnológico e os serviços corporativos da Agência;

g) disponibilidade de suporte técnico especializado;

h) possibilidade de manutenção e evolução das soluções durante a vigência contratual; e

i) aderência às necessidades institucionais de proteção da infraestrutura, dos usuários, dos serviços corporativos e das informações da ANTT.

19.1.6. A Equipe de Planejamento registra que os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, e os riscos envolvidos são administráveis.

19.2. Diante das análises realizadas, conclui-se que a contratação é plenamente viável sob os aspectos técnicos, operacional econômico e de mercado, sendo adequada e necessária para garantir a segurança da infraestrutura de TIC, a continuidade dos serviços institucionais e a proteção das informações.

19.3. Assim, recomenda-se o prosseguimento da contratação, em conformidade com os princípios da eficiência, economicidade e planejamento previstos na Lei nº 14.133/2021.

19.4. Considerando as informações do presente Estudo Técnico Preliminar, entende-se que a presente contratação configura-se tecnicamente VIÁVEL.

20. Responsáveis

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

JOSE EDSON DE SENA JUNIOR

Integrante Requisitante substituto

Assinou eletronicamente em 19/10/2026 às 15:17:07.

RONALD SEREJO REBELO

Integrante Técnico

KLEBER CAMPOS RODRIGUES FILHO

Autoridade Máxima de TIC

Assinou eletronicamente em 19/10/2026 às 18:35:00.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Apêndice A - Requisitos Mínimos da Solução.pdf (835.33 KB)