



AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019.

Histórico de Revisões

Data	Versão	Descrição	Autor
27/09/2022	1.0	Finalização da primeira versão do documento.	Equipe de planejamento da contratação
11/11/2022	2.0	Atendimento das recomendações do Parecer da Procuradoria	Equipe de planejamento da contratação

SUMÁRIO

1 – OBJETO DA CONTRATAÇÃO

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

3.3. Estimativa da demanda

3.4. Parcelamento da Solução de TIC

3.5. Resultados e Benefícios a Serem Alcançados

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.2. Requisitos de Capacitação

4.3. Requisitos Legais

4.4. Requisitos de Manutenção

4.5. Requisitos Temporais

4.6. Requisitos de Segurança e Privacidade

4.7. Requisitos Sociais, Ambientais e Culturais

4.8. Requisitos de Arquitetura Tecnológica

4.9. Requisitos de Projeto e de Implementação

4.10. Requisitos de Implantação

4.11. Requisitos de Garantia e Manutenção

4.12. Requisitos de Experiência Profissional

4.13. Requisitos de Formação da Equipe

4.14. Requisitos de Metodologia de Trabalho

4.15. Requisitos de Segurança da Informação e Privacidade

4.16. Outros Requisitos Aplicáveis

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

5.2. Deveres e responsabilidades da CONTRATADA

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.3. Mecanismos formais de comunicação

6.4. Manutenção de Sigilo e Normas de Segurança

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.2. Procedimentos de Teste e Inspeção

7.3. Níveis Mínimos de Serviço Exigidos

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.5. Do Pagamento

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

- 9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO
- 10 – DA VIGÊNCIA DO CONTRATO
- 11 – DO REAJUSTE DE PREÇOS
- 12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR
 - 12.1. Regime, Tipo e Modalidade da Licitação
 - 12.2 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência
 - 12.3 Critérios de Qualificação Técnica para a Habilitação
- 13 – SUBCONTRATAÇÃO E PARTICIPAÇÃO EM CONSÓRCIO
- 14 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

- 1. **OBJETO DA CONTRATAÇÃO**
 - 1.1. Contratação de empresa especializada para fornecimento de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.
- 2. **DESCRIÇÃO DA SOLUÇÃO DE TIC**
 - 2.1. **Bens e serviços que compõem a solução**

Item	Descrição	Métrica	Quantidade	CATSER	Valor Unitário Máximo Aceitável R\$	Valor Total Máximo Aceitável R\$
1	Subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.	Dispositivos	3.300	27456	505,54	1.668.282,00
VALOR TOTAL GLOBAL R\$						R\$ 1.668.282,00

- 3. **JUSTIFICATIVA PARA A CONTRATAÇÃO**
 - 3.1. **Contextualização e Justificativa da Contratação**
 - 3.1.1. O presente documento visa a contratação de empresa especializada para fornecimento de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.
 - 3.1.2. Atualmente a ANTT utiliza solução de antivírus tradicional (Windows Defender) que, diante da sofisticação dos ataques digitais e de novas ameaças que não se restringem apenas a artefatos maliciosos (códigos executáveis e artefatos embutidos em arquivos), não mais está apta a proteger o ambiente da Agência, visto que as assinaturas de ataque estão cada vez mais modernas e órgãos governamentais estão frequentemente sendo alvos de ataques cibernéticos. As tentativas de ataques são direcionadas e coordenadas, muitas vezes com a utilização de ferramentas do próprio sistema operacional, a exemplo de Fileless e Attacks, sendo cada vez mais comuns. Esses ataques têm causado prejuízos a grandes organizações ao redor do mundo, fazendo-se necessária, para Agência, a adição de mais uma camada de tecnologia que prevê a proteção para estes novos tipos de ataques digitais.
 - 3.1.3. A ANTT lida diariamente com uma grande diversidade de informações, das quais muitas são protegidas por lei. A presente contratação tem por objetivo atender demandas relacionadas à proteção de dispositivos, somada a outros esforços, utilizando como referência os padrões ABNT NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação.
 - 3.1.4. O processo de detecção e resposta a estes tipos de ameaças e tentativas de ataques sofisticados, necessita de tecnologias mais avançadas, baseadas em comportamento e inteligência artificial, capazes de detectar anomalias na execução de processos e operações que, muitas vezes, não são percebidas pelas soluções tradicionais.
 - 3.1.5. Diante disso, o cenário, exige um complemento da tecnologia atualmente utilizada pela ANTT, com soluções de nova geração, cujo aparato tecnológico seja mais inteligente e capaz de detectar estes desvios de comportamento no ambiente operacional, com capacidade de mitigação imediata e disponibilidade de instrumentos para investigação da causa raiz do problema, de maneira a proteger o ambiente de novos ataques.
 - 3.1.6. Ademais, foram realizados vários investimentos na concepção e adoção de sistemas internos estruturantes, além da aquisição de vários dispositivos como servidores de rede físicos e virtuais para serviços de e-mail, aplicações estruturantes, armazenamento de arquivos, além de inúmeras estações de trabalho, integrando seu uso em vários processos eletrônicos, melhorando a gestão, a transparência e a agilidade dos serviços prestados pela ANTT, e como consequência, torna-se importante proteger todos os dispositivos utilizados pela Agência, em especial a camada de estações de trabalho e servidores de rede corporativos, que são constantemente utilizados conectados à redes públicas e internas, ficando expostos a todo tipo de ameaças e infecções digitais oriundas da Internet.
 - 3.1.7. Diante do exposto, há a necessidade de contratação de solução de proteção de dispositivos e resposta a ataques cibernéticos, e possibilitar a atualização tecnológica atualmente em uso na Agência, aumentando a segurança e proteção do parque computacional e do ambiente de rede da ANTT.
 - 3.2. **Alinhamento aos Instrumentos de Planejamento Institucionais**
 - 3.2.1. A pretensa contratação encontra-se alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação da ANTT - PDTIC 2021-2024, ao Planejamento Estratégico Institucional - PEI, de acordo com o Mapa Estratégico da ANTT 2020-2030, e ao Plano Anual de Contratações - PAC 2022, conforme tabela abaixo:

Alinhamento ao Planejamento Estratégico Institucional - PEI			
Planejamento Estratégico ANTT - 2020-2030			
ID	Objetivo Estratégico		
OPG 4	Potencializar a capacidade de inovação e absorção de tecnologias de forma estruturada		
PR2	Aprimorar a disponibilidade, a qualidade e a integração das informações internas e externas		
Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC			
Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2021-2024			
ID	NECESSIDADE		
N7	Propor a modernização das tecnologias utilizadas nos sistemas de informação com uso de mecanismos inovadores		
N10	Aperfeiçoar os mecanismos e ambientes para assegurar alta disponibilidade e evolução tecnológica		
ID	Ação do PDTIC	ID	Meta do PDTIC associada
-	Definir padrões de qualidade com vistas a aprimorar a aquisição ou desenvolvimento das soluções	-	Implementar soluções com uso de inteligência artificial
-	Executar os serviços de gestão e manutenção de infraestrutura: dados em nuvem, site redundante, rede de dados, banco de dados, segurança.	-	Garantir disponibilidade das aplicações: 99%
Alinhamento ao Plano Anual de Contratações - PAC			
Item no PAC	Descrição	Aprovação	
3.42	Solução de proteção de dispositivos e resposta a ataques cibernéticos	Aprovado na Revisão do Planejamento Anual de Contratações - PAC 2022, nos termos da Deliberação nº 171, de 10 de maio de 2022.	

3.3. Estimativa da demanda

3.3.1. Para o correto dimensionamento da quantidade de subscrições a serem contratadas, a equipe de planejamento da contratação considerou os relatórios extraídos do Microsoft System Center Configuration Manager – SCCM, plataforma que reúne informações à respeito do ambiente computacional da ANTT. Pelo relatório, há um total de 2.472 devices, que correspondem às estações de trabalho (endpoints) atualmente ativas no ambiente de rede da Agência.

3.3.2. Também foram utilizados os relatórios extraídos da plataforma de virtualização - VSPHERE - utilizada para realizar a gestão dos servidores provisionados pela Agência. Neste relatório, evidencia um total de 940 servidores virtuais e 18 hosts físicos (um total de 958 servidores), sendo que desses, 800 estão em operação.

3.3.3. O quantitativo estimado a ser contratado refere-se ao somatório do número de estações de trabalho (endpoints) com o número total de servidores em operação.

3.3.4. Assim sendo, a estimativa da demanda deverá observar o quantitativo da tabela abaixo:

Item	Descrição	Métrica	Quantidade
1	Subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.	Dispositivo	3.300

3.4. Parcelamento da Solução de TIC

3.4.1. A solução é composta de um único item.

3.5. Resultados e Benefícios a Serem Alcançados

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

- Aumentar a segurança e proteção dos dispositivos que compõem o parque computacional e o ambiente de rede da ANTT, fornecendo à equipe de TI alertas para tomada de ações quanto a correção de infecções digitais que estejam sendo exploradas por atores maliciosos;
- Disponer de painel gráfico em nuvem em tempo real para acesso via browser possibilitando analisar informações das atividades de proteção e possíveis ataques explorando vulnerabilidades existentes nos dispositivos do ambiente computacional da ANTT;
- Melhorar o controle e a prevenção de ameaças que utilizam amplo espectro de técnicas de coleta de inteligência, não se restringindo a um único arquivo binário malicioso em qualquer dispositivo da ANTT;
- Aumentar a prevenção e a remediação em relação a ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia, e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais em todos os dispositivos da ANTT protegidos pela solução;
- Possibilitar o aumento da mitigação de riscos de ameaças em todo ambiente computacional da ANTT e seus dispositivos, que utilizam falhas recentes e não divulgadas dos sistemas operacionais (0-day exploits);
- Proporcionar em todos os dispositivos do ambiente da ANTT, a prevenção e remediação de tipos de ameaça que usam técnicas de dividir o ataque em diversas fases podendo, por exemplo, controlar um grande número de equipamentos para diferentes finalidades, de modo que diferentes partes da infraestrutura-alvo sejam utilizadas em cada uma das fases do possível ataque;
- Reduzir o risco de ameaças que utilizam técnicas de persistência com o direcionamento do ataque conduzido por uma interação e um monitoramento contínuo, até que se alcance um objetivo de invasão e ataque, não buscando apenas oportunidades eventuais nos dispositivos da ANTT;
- Evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers, reduzindo o risco dos dispositivos, serviços e sistemas tecnológicos da ANTT serem acessados sem autorização;
- Proporcionar consultas para auditoria por meio de Dashboard das detecções mais recentes, a quantidade de novas detecções e as que aconteceram por táticas nos últimos 30 dias, sendo possível reportar de forma agrupada para os dispositivos do ambiente de rede da ANTT.

- j) Prover relatórios de todas as conexões remotas realizadas desde a console de gerenciamento até o dispositivo final gerenciado, contendo informações detalhadas de sua utilização, garantindo o não-repúdio e/ou exclusão de informações;
- k) Prover a melhoria e automação dos fluxos de trabalho, onde estejam sendo realizados manualmente pelas equipes de TI da ANTT, reduzindo os prazos de execução e custos operacionais;
- l) Ampliação da visibilidade, transparência e colaboração corporativa que trazem excelência operacional, alinhamento entre as áreas de TI e Negócio da ANTT e a qualidade de atendimento a seus clientes internos e externos.

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. A presente demanda visa a contratação de empresa especializada para o fornecimento de licenças/subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento, visando prover ao Agência Nacional de Transporte Terrestre - ANTT a proteção de seus ativos, da eficiência e do controle de qualidade de suas operações, aumentando assim a segurança tecnológica no ambiente computacional da ANTT.

4.1.2. Contratar uma solução que possibilite sua administração de forma centralizada a partir de sua console única de administração em nuvem, possibilitando um gerenciamento único das partes integradas necessárias a seu funcionamento, com características de controle e correção de possíveis vírus digitais baseado em comportamento e inteligência artificial, com capacidade de resposta aos incidentes que ocorrerem, privilegiando fazer com menos estrutura, reduzindo custos com sala-cofre, site-backup, infraestrutura de hardware, software e recursos humanos internos e terceirizados que estariam envolvidos em sua sustentação e manutenção, além da redução dos custos com depreciação e atualização de versões e pré-requisitos de funcionamento.

4.1.3. Continuidade de Negócio – Aquisição de solução que aumente a segurança e proteção dos dispositivos que compõem o parque computacional e o ambiente de rede da ANTT, fornecendo à equipe de TI alertas para tomada de ações quanto a correção de vulnerabilidades e infecções digitais.

4.1.4. A solução deverá possuir painel gráfico em nuvem em tempo real para acesso via browser possibilitando analisar informações das atividades de proteção e possíveis ataques e/ou vulnerabilidades encontradas nos dispositivos do ambiente computacional da ANTT.

4.1.5. A solução deverá aumentar a prevenção e a remediação em relação a ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais em todos os dispositivos da ANTT protegidos pela solução.

4.1.6. A solução deverá melhorar o controle e a prevenção de ameaças que utilizam amplo espectro de técnicas de coleta de inteligência, não se restringindo a um único arquivo binário malicioso em qualquer dispositivo da ANTT, Windows, Linux.

4.1.7. A solução deverá possibilitar o aumento da mitigação de riscos de ameaças em todo ambiente computacional da ANTT e seus dispositivos, que utilizam falhas recentes e não divulgadas dos sistemas operacionais (0-day exploits).

4.1.8. A solução deverá proporcionar em todos os dispositivos do ambiente da ANTT, a prevenção e remediação de tipos de ameaça que usam técnicas de dividir o ataque em diversas fases podendo, por exemplo, controlar um grande número de equipamentos para diferentes finalidades, de modo que diferentes partes da infraestrutura-alvo sejam utilizadas em cada uma das fases do possível ataque.

4.1.9. A solução deverá reduzir o risco de ameaças que utilizam técnicas de persistência com o direcionamento do ataque conduzido por uma interação e um monitoramento contínuo, até que se alcance um objetivo de invasão e ataque, não buscando apenas oportunidades eventuais nos dispositivos da ANTT.

4.1.10. A solução deverá prover a melhoria e automação dos fluxos de trabalho, onde seja possível deixar de serem realizados manualmente pelas equipes de TI da ANTT, reduzindo os prazos de execução e custos operacionais e aumentar a economia de recursos pela simplificação dos processos, redução no consumo de recursos humanos e melhoria nos fluxos de trabalho, em especial por passar a não ser mais necessário administrar vacinas pois a tecnologia pretendida é baseada em inteligência artificial.

4.1.11. A solução deverá possuir uma console de administração que seja acessível em qualquer ponto da rede da ANTT, inclusive se houver conexão a redes públicas sem a necessidade de uma conexão privada (VPN).

4.1.12. A solução deverá possibilitar sua administração totalmente em nuvem sem a necessidade de instalar ferramental local para seu gerenciamento, sendo local apenas os sensores/agentes.

4.1.13. A solução deverá ser em nuvem e deverá necessariamente cumprir pelo menos os requisitos exigidos no item 5 da certificação PCI-DSS V3.2 (Padrão de segurança de dados do setor de cartões de pagamento para organizações de qualquer local do mundo que lidam com cartões de crédito de marca das principais bandeiras/marcas de cartões).

4.2. Requisitos de Capacitação

4.2.1. A presente contratação prevê transferências de conhecimento que poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências da ANTT, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da ANTT, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução fornecida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

4.2.2. Serão solicitadas no mínimo, 2 (duas) workshops de transferência de conhecimento, sendo uma na implantação da solução, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente, e no máximo 1 (uma) workshop de transferência de conhecimento por mês caso a equipe da ANTT entenda que seja necessário.

4.3. Requisitos Legais

4.3.1. [Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019](#) - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4.4. Requisitos de Manutenção

4.4.1. Da Manutenção preventiva

4.4.1.1. A manutenção preventiva será destinada a atualizar os componentes de software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução.

4.4.1.2. Durante a manutenção preventiva a CONTRATADA deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da ANTT decidirá sobre a aplicação ou não das recomendações.

4.4.1.3. A manutenção preventiva deverá ser executada conforme demanda da ANTT.

4.4.1.4. Deverá ser gerado um relatório técnico em 2 (duas) vias a cada manutenção preventiva, que deverá ser entregue até 5 (cinco) dias após a visita da CONTRATADA, para a equipe técnica da ANTT.

4.4.1.5. As visitas para prestação do serviço de manutenção preventiva, independentemente da quantidade necessária, não implicarão em custos adicionais para a ANTT e deverão estar inclusas no custo da garantia técnica.

4.4.2. Da manutenção corretiva

4.4.2.1. A manutenção preventiva será destinada a atualizar os componentes de software e a realizar quaisquer operações que evitem uma parada parcial ou total da solução.

4.4.2.2. Durante a manutenção preventiva a CONTRATADA deverá analisar a solução, sua condição atual de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da ANTT decidirá sobre a aplicação ou não das recomendações.

4.4.2.3. A manutenção preventiva deverá ser executada conforme demanda da ANTT.

4.4.2.4. Deverá ser gerado um relatório técnico em 2 (duas) vias a cada manutenção preventiva, que deverá ser entregue até 5 (cinco) dias após a visita da CONTRATADA, para a equipe técnica da ANTT.

4.4.2.5. As visitas para prestação do serviço de manutenção preventiva, independentemente da quantidade necessária, não implicarão em custos adicionais para a ANTT e deverão estar inclusas no custo da garantia técnica.

4.5. Requisitos Temporais

4.5.1. Na forma da tabela abaixo:

Descrição	Prazo
Reunião Inicial	Em até 5 (cinco) dias úteis a contar da assinatura do CONTRATO.
Instalação e configuração da solução de proteção de dispositivos	Em até 15 (quinze) dias corridos a contar da data de emissão da(s) Ordem(ns) Serviço.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A solução em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com no mínimo os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes).

4.6.2. A solução deverá incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques.

4.6.3. A solução deverá ser capaz de detectar *Adware* e programas potencialmente indesejados.

4.6.4. A solução deverá permitir bloqueio de scripts e comandos em Powershell considerados suspeitos e também deverá permitir bloqueio automático de processos suspeitos.

4.6.5. A solução deverá permitir bloqueios baseados em análise do centro de inteligência do fabricante em nuvem e deverá permitir bloqueio de operações em registro suspeitos, além de permitir que arquivos maliciosos possam ser movidos para uma área de quarentena.

4.6.6. A solução deverá possuir integração com o Windows Security Center da Microsoft para ser reconhecido como uma solução de proteção válida para *antimalware*.

4.6.7. A solução deverá ser capaz de detectar *malwares* do tipo *Ransomware* com base em, no mínimo, os comportamentos de Deletar backups; Operações em excesso ao sistema de arquivos; Criptografia de arquivos; Processos associados a malwares de ransomware Cryptowall, Wannacry, Locky; além de ser capaz de detectar exploração baseado em, no mínimo, os comportamentos de criação de processos suspeitos originados de navegadores; detecção de comprometimento de servidores Web através de webshell; detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução; injeção de código não esperada de um processo a outro; e execução de JavaScript através do executável Rundll32.

4.6.8. A solução deverá possuir inteligência de ameaças e deverá mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, país de origem da campanha e última atividade, além de fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de entrega e breve descrição da campanha e deve associar, quando pertinente, detecções presentes no ambiente à campanha de ataque.

4.6.9. A solução deverá prover, integrada à console de administração, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros.

4.6.10. A solução deverá se integrar ao agente/sensor instalado nos dispositivos para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução, que deverá emular execução, no mínimo, nos sistemas operacionais Windows 7 (32 e 64 bits), Windows 10, Linux Ubuntu, e Android.

4.6.11. A solução deverá prover *Dashboard* trazendo as detecções mais recentes e o número de novas detecções por táticas nos últimos 30 dias e deverá ter a capacidade de reportar as detecções de forma agrupada, como por exemplo por tática, além de ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo, de forma a reportar as detecções, permitindo filtrar minimamente com base pelo menos nos filtros de Severidade, Tática, Técnica, Usuário, Host, Tipo de sistema operacional, Versão do sistema operacional, Última hora, Último dia, Última semana, Últimos 30 dias, Nome de arquivo e Hash do processo.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na [Instrução Normativa SLTI/MP nº 1/2010](#) e [Decreto nº 7.746/2012](#), da Casa Civil, da Presidência da República.

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

- baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;
- preferências para materiais, tecnologias e matérias-primas de origem local;
- maior eficiência na utilização de recursos naturais como água e energia;
- maior geração de empregos, preferencialmente com mão de obra local;
- maior vida útil e menor custo de manutenção de bens;
- uso de inovações que reduzam a pressão sobre recursos naturais;
- origem sustentável dos recursos naturais utilizados nos bens e serviços;
- adotar práticas de gestão que garantam os direitos trabalhistas e o atendimento às normas internas e de segurança e medicina do trabalho para seus empregados;
- administrar situações emergenciais de acidentes com eficácia, mitigando os impactos aos empregados, colaboradores, usuários e ao meio ambiente;
- conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e à saúde dos trabalhadores e envolvidos na prestação dos serviços;
- realizar um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de redução de consumo de água e redução da produção de resíduos sólidos, observadas as normas ambientais vigentes;
- disponibilizar os Equipamentos de Proteção Individual (EPIs), quando aplicável, para a execução das atividades de modo confortável, seguro e de acordo com as condições climáticas, favorecendo a qualidade de vida no ambiente de trabalho;
- orientar sobre o cumprimento, por parte dos funcionários, das Normas Internas e de Segurança e Medicina do Trabalho, tais como prevenção de incêndio nas áreas da prestação de serviço, zelando pela segurança e pela saúde dos usuários;
- respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;
- orientar seus empregados para a destinação dos resíduos recicláveis descartados aos devidos coletores de resíduos recicláveis existentes nas dependências da ANTT.

4.7.3. A licitante deverá apresentar Declaração de Sustentabilidade Ambiental, conforme modelo constante deste Termo de Referência (**APÊNDICE “D”**), a ser apresentado na fase de aceitação da proposta.

4.7.4. A exigência visa atender aos dispositivos normativos, acima enumerados, bem como demais normativos acerca dos critérios de sustentabilidade socioambiental, de forma a estabelecer que a licitante promova ações ambientais por meio de treinamento de seus colaboradores, pela conscientização de todos os envolvidos na prestação dos serviços, visando o cumprimento das ações estabelecidas neste Termo de Referência, que se estenderão na gestão contratual, refletindo na responsabilidade da Administração no desempenho do papel de consumidor potencial e na responsabilidade ambiental e socioambiental entre as partes.

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. A ANTT disponibilizará máquinas virtuais para o caso de solução baseada em software sem sistema operacional, sendo os demais custos relativos à implementação da solução a cargo da CONTRATADA.

4.8.2. Licenças - Ambiente computacional da ANTT:

- I - Sistema Operacional: Windows 10 (64 bits);
- II - Memória RAM instalada: 8 GB;
- III - Processador: Intel Core i5 3,50 GHz.

4.8.3. A implantação da solução adquirida deverá permitir a atualização tecnológica e alinhamento em relação a padrões, formatos, versões e tecnologias comuns para a execução das atividades técnicas da Agência, com qualidade e produtividade suficientes, em conformidade legal às normas brasileiras de uso de licenciamento de programas de computador.

4.8.4. Deverá permitir a atualização continuada de software específicos e de suporte técnico ao seu uso, incluindo atualização de versões e evoluções de segurança.

4.9. **Requisitos de Projeto e de Implementação**

4.9.1. Para a implantação e operacionalização das atividades definidas neste Termo de Referência, a CONTRATADA deverá observar os padrões e diretrizes vigentes nos ambientes da ANTT, tais como técnicas, métodos, arquiteturas e documentação, dentre outros.

4.9.2. Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários e acessos necessários de acordo com as políticas e diretrizes de segurança da agência.

4.9.3. As atividades de instalação e configuração inicial da solução, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da ANTT.

4.9.4. Para esta etapa a ANTT não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe acompanhará a ativação dos serviços, da console e a integração com os dispositivos da ANTT, mantendo o alinhamento com o planejamento estratégico de TI da ANTT.

4.10. **Requisitos de Implantação**

4.10.1. Durante a etapa de implantação e migração, a solução fornecida pela CONTRATADA deverá ser colocada em plena operação, em condições reais de produção, e sua equipe deverá estar presente, nos horários de testes, implantação e migração, definidos pela ANTT, e estes horários poderão ser horário comercial, período noturno ou final de semana.

4.10.2. A solução deverá ser instalada e configurada a integração com os dispositivos necessários a serem protegidos, em no máximo 15 (quinze) dias contados da data de assinatura do Contrato, e durante esta etapa, a equipe da CONTRATADA deverá estar de forma remota, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários necessários para os acessos necessários de acordo com as políticas e diretrizes de segurança da ANTT, sendo que as atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da equipe da ANTT e para esta ou qualquer outra etapa a ANTT não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe acompanhará a ativação dos serviços, da console e a integração com os dispositivos.

4.11. **Requisitos de Garantia e Manutenção**

4.11.1. A CONTRATADA deverá fornecer suporte direto do fabricante da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante se necessário, além do nível de suporte que deverá ser prestado pela CONTRATADA em conjunto, conforme previsto neste Termo de Referência seus Apêndices.

4.11.2. A CONTRATADA deverá prestar, pelo período da vigência contratual, Suporte Técnico com Operação Assistida e Transferência de Conhecimento, que deverão ser do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, sendo realizado por profissionais especializados, e devendo cobrir todo e qualquer defeito ou demanda apresentada.

4.11.3. Os serviços de suporte e manutenção consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e atualizações de versões para correções de eventuais problemas identificados.

4.11.4. As atividades de suporte técnico serão realizadas, a critério do ANTT, em seu ambiente, a partir da assinatura do Contrato e durante toda sua vigência contratual.

4.11.5. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração dos dispositivos e desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

- a) Orientação sobre acesso, o uso, a configuração, a instalação de agentes e/ou sensores nos dispositivos, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do FABRICANTE da solução;
- b) Orientação quanto às melhores práticas para implementação e integração da solução no ambiente da ANTT;
- c) Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto nos agentes e/ou sensores já instalados no ambiente da ANTT;
- d) Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas nos dispositivos protegidos e monitorados pela console central;
- e) Aplicação de melhores práticas para implementação dos produtos de software adquiridos;
- f) Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam;
- g) Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas;
- h) Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias novas integrações;
- i) Identificação de melhorias e respectivo tratamento (melhoria de parametrização);
- j) Parametrização da solução, de acordo com as regras e políticas disponíveis em sua console única e definidas pela ANTT;
- k) Apoio para execução de procedimentos de atualização para novas versões dos agentes e/ou sensores instalados nos dispositivos;
- l) Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário;
- m) Suporte avançado para estratégia e planejamento de migrações e adequações nos agentes e sensores instalados nos dispositivos protegidos pela solução;
- n) Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe da ANTT;

o) Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes;

4.11.6. A CONTRATANTE poderá solicitar durante toda a vigência contratual do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe, para isso serão abertos chamados com severidade “4” classificado como “baixa”.

4.11.7. As transferências de conhecimento poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências da ANTT, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da ANTT, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução fornecida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

4.11.8. Serão solicitadas no mínimo, 2 (duas) workshops de transferência de conhecimento, sendo uma na implantação da solução, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente, e no máximo 1 (uma) workshop de transferência de conhecimento por mês caso a equipe da ANTT entenda que seja necessário.

4.11.9. Para os casos em que houver alguma mudança significativa que reflita na operação da solução ou reflita nos agentes e/ou sensores instalados nos dispositivos, a CONTRATADA deverá transferir este conhecimento para equipe sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4”.

4.11.10. Os serviços de operação assistida poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverão ser realizados nas dependências da ANTT, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da ANTT, de modo que os trabalhos possam ser realizados com qualidade e eficácia, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

4.11.11. Será solicitado no mínimo, 1 (uma) sessão de operação assistida por trimestre, e no máximo 1 (uma) sessão por mês, devendo ocorrer logo após a implantação da solução, para possibilitar qualquer nova análise de funcionamento, configuração e/ou modificação necessárias nas implementações e integrações já realizadas, de modo que o funcionamento se mantenha sempre atualizado, em produção e devidamente funcional e integrado aos dispositivos pertencentes ao ambiente da ANTT.

4.11.12. O serviço deverá ocorrer durante toda a vigência contratual, e deverá ser disponibilizado pela CONTRATADA um sistema de acompanhamento e controle de chamados onde eles serão registrados com acesso liberado para cada integrante da equipe da ANTT que será informado no início da vigência contratual.

4.11.13. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe da ANTT.

4.11.14. Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Severidade	Descrição	Prazo máximo de início de atendimento remoto	Prazo máximo para a solução remota	Prazo máximo da solução
Crítica (Severidade 1)	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 8 (oito) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após abertura do chamado remoto.
Alta (Severidade 2)	Impacto de alta significância relacionado à utilização do ambiente: ocorrência de indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias após abertura do chamado remoto.
Normal (Severidade 3)	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto.	Até 48 (quarenta e oito) horas após a abertura do chamado remoto.	Até 8 (oito) dias após abertura do chamado remoto.
Baixa (Severidade 4)	Consulta e/ou dúvida técnica e/ou transferência de conhecimento.	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após a abertura do chamado remoto.	Até 10 (dez) dias após a abertura do chamado remoto.

4.11.15. Não haverá limite para o número de chamados de suporte técnico.

4.11.16. O nível de severidade será atribuído pela equipe autorizada da ANTT no momento da abertura do chamado.

4.11.17. Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que a ANTT estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de protocolo/número de abertura do mesmo.

4.11.18. Uma vez que a solução estará em produção e funcionando em nuvem, as atividades relacionadas a correções ou atualizações da console que necessitem indisponibilidade do ambiente, sem prejuízo para o funcionamento dos dispositivos já gerenciados pela solução, deverão ser notificadas à ANTT com antecedência mínima de 1 (um) dia útil.

4.11.19. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e caso seja definido pela ANTT poderão ser aplicadas glosas conforme tabela especificada no item 7.3 deste Termo de Referência.

4.12. Requisitos de Experiência Profissional

4.12.1. A CONTRATADA deverá utilizar profissionais devidamente capacitados e habilitados para o objeto especificado neste Termo de Referência, impondo-lhes rigoroso padrão de qualidade, segurança e eficiência.

4.13. Requisitos de Formação da Equipe

4.13.1. A execução dos serviços deve ser realizada pela CONTRATADA por meio de profissional certificado pelo fabricante da solução sem custos adicionais para a ANTT, durante o período de garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual, podendo ser solicitada a qualquer momento.

4.14. **Requisitos de Metodologia de Trabalho**

4.14.1. Realização de Reunião Inicial previamente à entrega da solução e à execução dos serviços de instalação.

4.14.2. Realização de reuniões entre a ANTT e CONTRATADA para discussão de assuntos referentes às instalações em execução e acompanhamento do cronograma.

4.14.3. Execução das etapas demandadas e posterior aceite/rejeição pela equipe de fiscalização da contratação e o Gestor do Contrato.

4.14.4. Profissionais qualificados da CONTRATADA deverão realizar o repasse de conhecimento para operacionalização e configuração da solução fornecida, direcionada à equipe técnica da ANTT.

4.15. **Requisitos de Segurança da Informação e Privacidade**

4.15.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da ANTT e aos padrões estabelecidos pela ISO 17799.

4.15.2. A solução deve ser mantida atualizada para assegurar sua disponibilidade e integridade continuadas.

4.15.3. O serviço deve passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor e acordados com a CONTRATADA.

4.15.4. Devem ser mantidos registros sobre todas as falhas ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas.

4.15.5. Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.

4.15.6. A CONTRATADA se compromete a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.

4.15.7. A CONTRATADA deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados pelo prestador de serviços, observadas as seguintes diretrizes:

4.15.7.1. Garantia de aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados;

4.15.7.2. Garantia que, em qualquer hipótese, a Administração tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços;

4.15.8. Vedado o uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço.

4.15.9. Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção.

4.15.10. Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

4.15.11. A CONTRATADA deverá seguir as normas internas de segurança da informação da ANTT, bem como suas atualizações.

4.15.12. 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 ANTT a tais documentos.

4.15.13. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da ANTT sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

4.15.14. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela ANTT 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 ANTT ou acessadas a partir dos seus equipamentos poderão ser auditadas.

4.15.15. 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 ANTT.

4.16. **Outros Requisitos Aplicáveis**

4.16.1. Não se aplica.

5. **RESPONSABILIDADES**

5.1. **Deveres e responsabilidades da CONTRATANTE**

a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b) Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

c) Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

a) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

b) Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

c) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

d) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

e) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

f) Verificar, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e, posterior, recebimento definitivo.

5.2. **Deveres e responsabilidades da CONTRATADA**

a) Indicar formalmente e por escrito, no prazo máximo de 5 (cinco) dias corridos após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

c) Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

d) Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

- e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- f) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- g) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- h) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;
- i) Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
- j) Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;
- k) Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

- 5.3.1. Não se aplica.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. Da reunião de alinhamento

6.1.1.1. Deverá ser realizada reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e Anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

6.1.1.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato na ANTT e o Representante da CONTRATADA.

6.1.1.3. A reunião realizar-se-á na ANTT em até 05 (cinco) dias úteis a contar da data de assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato na ANTT.

6.1.1.4. Nessa reunião a CONTRATADA deverá apresentar oficialmente seu Preposto, além de fornecer as respectivas comprovações acerca dos requisitos de qualificação exigidos para os seus profissionais na execução do Objeto.

6.1.1.5. Todos os entendimentos da reunião de alinhamento deverão constar da Ata de reunião a ser lavrada pelo Gestor do Contrato na ANTT e assinada por todos os participantes.

6.1.1.6. A CONTRATADA cumprirá as instruções complementares da ANTT quanto à execução e horário de realização do serviço, permanência e circulação de seu(s) técnico(s) nas dependências da ANTT e unidades vinculadas.

6.1.2. Da Ordem de Serviço

6.1.2.1. A execução dos serviços e o fornecimento dos bens serão realizados mediante a abertura de Ordem de Serviço (OS) e autorização do Gestor do Contrato.

6.1.2.2. A OS registrará as etapas, os prazos e o detalhamento dos serviços de entrega e ativação, bem como demais informações necessárias para a execução dos serviços por parte da CONTRATADA.

6.1.2.3. Após aprovação das demandas, o Gestor do Contrato encaminhará a OS para a CONTRATADA, bem como as informações necessárias para sua execução.

6.1.2.4. Cada demanda deverá ser executada atendendo as especificações e condições constantes deste Termo de Referência e melhores práticas, além das que constarem da OS.

6.1.3. Do local de entrega do objeto e execução dos serviços

6.1.3.1. O local de entrega, instalação e configuração será na:

- a) Sede da Agência Nacional de Transportes Terrestres - ANTT, localizada no Setor de Clubes Esportivos Sul - SCES, lote 10, trecho 03, Projeto Orla Polo 8 - Brasília - DF, CEP: 70200-003.

6.1.4. Do prazo de execução

6.1.4.1. A CONTRATADA deverá observar os prazos de execução descrito na subitem 4.5. deste TERMO DE REFERÊNCIA.

6.1.5. Da Gestão do Contrato

6.1.5.1. A ANTT, por meio de representantes nomeados, fiscalizará a execução do contrato, não importando essa fiscalização em redução ou supressão da responsabilidade da CONTRATADA por eventual erro, falha ou omissão, exceto se decorrentes de determinações emanadas da ANTT, das quais a CONTRATADA tenha discordado por escrito.

6.1.5.2. Para isso, a ANTT registrará em relatório as deficiências verificadas na execução dos serviços, encaminhando notificações à CONTRATADA, para a imediata correção das irregularidades apontadas, sem prejuízo da aplicação das penalidades previstas neste Termo de Referência.

6.1.5.3. Objetivando assegurar à ANTT eficiente coordenação, a CONTRATADA obriga-se a indicar um representante e seu substituto eventual, para responder, perante a ANTT pelo gerenciamento técnico e operacional do contrato, até o total cumprimento das obrigações assumidas.

6.1.6. Dos papéis e responsabilidades

6.1.6.1. Pela Agência Nacional de Transportes Terrestres - ANTT

- a) **Gestor do Contrato:** Servidor com capacidade gerencial, técnica e operacional, relacionada ao processo de gestão do contrato.
- b) **Fiscal Requisitante:** Servidor representante da SUTEC, indicado pela autoridade competente, responsável em fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.
- c) **Fiscal Técnico:** Servidor representante da SUTEC, indicado pela autoridade competente, responsável em fiscalizar tecnicamente o contrato.
- d) **Fiscal Administrativo:** Servidor representante da área administrativa, indicado pela autoridade competente, responsável por fiscalizar os aspectos administrativos do contrato.

6.1.6.2. Pela CONTRATADA

- a) **Preposto:** Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à ANTT, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

6.1.7. Interação entre a ANTT e CONTRATADA

6.1.7.1. Reuniões Periódicas

- a) Deverão ser realizadas reuniões periódicas para encerramento das etapas previstas no Termo de Referência, bem como recebimento dos serviços e produtos definidos.
- b) As reuniões periódicas deverão ser realizadas nas instalações da sede da ANTT, em Brasília-DF, com a participação, no mínimo, do Gestor e fiscais do Contrato na ANTT e do Representante da CONTRATADA.
- c) Todos os entendimentos das reuniões periódicas deverão constar da Ata de reunião a ser lavrada pelo Gestor do Contrato na ANTT e assinada por todos os participantes.

6.1.7.2. Reuniões de Validações

- a) Deverá ser realizada uma reunião com o objetivo de verificar se as expectativas do Contrato foram alcançadas, de identificar possíveis ocorrências não desejáveis e de consolidar lições aprendidas.
- b) Deverão participar dessa reunião, no mínimo, o Gestor e Fiscais do Contrato na ANTT e o Representante da CONTRATADA.
- c) A reunião realizar-se-á em até 15 (quinze) dias consecutivos e contados para o encerramento da vigência do Contrato, conforme agendamento efetuado pelo Gestor do Contrato na ANTT.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1. Não se aplica.

6.3. Mecanismos formais de comunicação

6.3.1. A comunicação entre a ANTT e a CONTRATADA, para fins de encaminhamento de Ordens de Serviço / Ordens de Fornecimento de Bens ou outro documento, ocorrerá sempre via Preposto, ou seu substituto, designado pela CONTRATADA.

6.3.2. São instrumentos formais de comunicação entre a ANTT e a CONTRATADA:

- a) Ordens de Serviço;
- b) Termos de Recebimento;
- c) Ofícios;
- d) Relatórios e Atas de Reunião;
- e) E-mail institucional/corporativo;
- f) Ferramenta Microsoft Teams ou similar em uso pela ANTT;
- g) Sistema Eletrônico de Informações - SEI (<https://portal.antt.gov.br/sei>);
- h) Demais Termos previstos no instrumento convocatório.

6.4. Manutenção de Sigilo e Normas de Segurança

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

6.4.2. O **Termo de Compromisso e Manutenção de Sigilo**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos **APÊNDICES "H" e "I"**.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

7.1.2. No prazo de até 5 (cinco) dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual.

7.1.3. O recebimento provisório será realizado pelo fiscal técnico do contrato, conforme inciso I, art. 33 da IN SGD/ME nº 1/2019, podendo ainda ser realizado por fiscal setorial ou por equipe de fiscalização designada, após a entrega da documentação acima, da seguinte forma:

7.1.4. A ANTT realizará inspeção minuciosa de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar as revisões finais que se fizerem necessários.

7.1.5. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao Gestor do Contrato.

7.1.6. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.1.7. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.1.8. No prazo de até 10 (dez) dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou a equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, e encaminhá-lo ao Gestor do Contrato.

7.1.9. Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao Gestor e Fiscal Requisitante do Contrato para recebimento definitivo.

7.1.10. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

7.1.11. Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

7.1.12. No prazo de até 15 (quinze) dias corridos a partir do recebimento provisório dos serviços, o Fiscal Requisitante e o Fiscal Técnico do Contrato deverão providenciar o recebimento definitivo, conforme inciso VIII, art. 33 da IN SGD/ME nº 1/2019, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

7.1.13. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções; e

7.1.14. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas.

7.1.15. O Gestor do Contrato, com base nas informações produzidas a partir do Termo de Recebimento Definitivo confeccionado pelos Fiscais Requisitante e Técnico do Contrato, comunicará a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização, com base no Instrumento de Medição de Resultado (IMR), Níveis Mínimos de Serviço (NMS), Indicadores de Medição e Resultados, ou instrumentos equivalentes.

7.1.16. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

7.1.17. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo de até 7 (sete) dias úteis, às custas da Contratada, sem prejuízo da aplicação de penalidades.

7.2. Procedimentos de Teste e Inspeção

7.2.1. A ANTT poderá, se julgar necessário, realizar inspeções e diligências a fim de garantir que a licitante vencedora esteja em condições de fornecer os produtos/serviços pretendidos de acordo com a qualidade exigida pela Agência.

7.3. Níveis Mínimos de Serviço Exigidos

7.3.1. Os níveis mínimos de serviço acordados e os descontos em favor da ANTT pelo respectivo descumprimento encontram-se definidos na tabela a seguir:

INDICADOR DE ATENDIMENTO DE CHAMADO TÉCNICO		
Tópico	Descrição	
Finalidade	Medir o tempo de atendimentos dos chamados técnicos, de acordo com o nível de severidade	
Meta a cumprir	Severidade 1 - CRÍTICA ≤ 72 horas	A meta definida visa garantir o atendimento dos chamados técnicos dentro do prazo previsto.
	Severidade 2 - ALTA ≤ 120 horas	
	Severidade 3 - NORMAL ≤ 192 horas	
	Severidade 4 - BAIXA ≤ 240 horas	
Instrumento de medição	Registro de protocolo do chamado técnico	
Forma de acompanhamento	Relatório mensal de registro de chamados técnicos O relatório de atendimento solicitado deverá ser extraído do próprio sistema de atendimento e apresentado na sua forma original, bem como na forma de relatório gerencial, para facilitar sua análise. O modelo do relatório pode ser definido em conjunto entre a CONTRATADA e a ANTT na reunião de alinhamento.	
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	IAT = TAT – TMA Onde: IAT - Indicador de Atendimento Técnico TAT - Tempo de Atendimento Técnico - corresponde ao tempo que os técnicos da CONTRATADA utilizaram para atendimento e resolução do problema TMA - Tempo Máximo de Atendimento - corresponde ao tempo máximo para atendimento e resolução do problema, de acordo com o nível de severidade	
Observações	Obs1: Serão excluídos da contagem de tempo de atraso de atendimento técnico, os decorrentes e dependentes de ações por parte da ANTT. Obs2: Se o resultado do indicador for positivo, representará o tempo de atraso no atendimento.	
Início de Vigência	A partir do registro de protocolo do chamado técnico	
Faixas de ajuste no pagamento e Sanções	0,7% sobre o valor mensal do contrato, por hora ou fração, em caso de atraso na resolução de chamados com severidade CRÍTICA, limitada a incidência a 72 (setenta e duas) horas	
	0,5% sobre o valor mensal do contrato, por hora ou fração, em caso de atraso na resolução de chamados com severidade ALTA, limitada a incidência a 120 (cento e vinte) horas	
	0,3% sobre o valor mensal do contrato, por hora ou fração, em caso de atraso na resolução de chamados com severidade NORMAL, limitada a incidência a 192 (cento e noventa e duas) horas	
	0,1% sobre o valor mensal do contrato, por hora ou fração, em caso de atraso na resolução de chamados com severidade BAIXA, limitada a incidência a 240 (duzentos e quarenta) horas	

7.3.2. Os Níveis Mínimos de Serviço são critérios para aferir e avaliar os diversos indicadores relacionados com os serviços contratados.

7.3.3. No Nível Mínimo de Serviço está definida a maneira pela qual estes fatores serão avaliados e as deduções a serem aplicadas na fatura mensal, quando o serviço prestado não alcançar o nível mínimo aceitável.

7.3.4. A aferição e a avaliação dos serviços prestados dar-se-á mensalmente pela ANTT e serão apresentadas por meio de relatório apresentado pela CONTRATADA.

7.3.5. A identificação de inconsistências entre os indicadores apresentados e os indicadores apurados pela fiscalização da ANTT, configura-se como não cumprimento do Nível Mínimo de Serviço, sendo neste caso aplicada as glosas previstas neste Termo de Referência, levando-se em consideração a dedução no pagamento da fatura estipulada na tabela de indicadores de níveis mínimos de serviço.

7.3.6. A simples aplicações de glosas por descumprimento do acordo de nível de serviço não exime a CONTRATADA de outras sanções estabelecidas neste Termo de Referência.

7.4. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.4.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993, a CONTRATADA que:

- falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas na contratação;
- ensejar o retardamento da execução do objeto;
- fraudar na execução do contrato;
- comportar-se de modo inidôneo; ou
- cometer fraude fiscal.

7.4.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções, na forma da tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 2% sobre o valor total do Contrato.

2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 10% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 10% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 2 (dois) dias úteis.	Multa de 1% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 7 dias úteis.
		Após o limite de 7 dias úteis, aplicar-se-á multa de 10 do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 3% do valor total do Contrato.

7.4.3. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

7.4.3.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

7.4.3.2. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados;

7.4.3.3. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação.

7.4.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

7.4.5. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

7.4.6. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do contratada, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

7.4.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.4.9. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

7.4.10. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

7.4.11. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.4.12. As penalidades serão obrigatoriamente registradas no SICAF.

7.5. Do Pagamento

7.5.1. O pagamento será efetuado pela ANTT no prazo de 30 (trinta) dias, contados do recebimento da Nota Fiscal/Fatura.

- 7.5.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da [Lei nº 8.666/1993](#), deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da [Lei nº 8.666/1993](#).
- 7.5.3. A emissão da Nota Fiscal/Fatura será **PRECEDIDA DO RECEBIMENTO DEFINITIVO** do serviço, conforme este Termo de Referência.
- 7.5.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da [Lei nº 8.666/1993](#).
- 7.5.5. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da [Instrução Normativa nº 3, de 26 de abril de 2018](#).
- 7.5.6. O setor competente para proceder o pagamento verificará se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:
- 7.5.6.1. o prazo de validade;
- 7.5.6.2. a data da emissão;
- 7.5.6.3. os dados do contrato e do órgão contratante;
- 7.5.6.4. o período de prestação dos serviços;
- 7.5.6.5. o valor a pagar; e
- 7.5.6.6. eventual destaque do valor de retenções tributárias cabíveis.
- 7.5.7. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a ANTT;
- 7.5.8. Nos termos do item 1, do Anexo VIII-A da [Instrução Normativa SEGES/MP nº 05/2017](#), será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:
- 7.5.8.1. não produziu os resultados acordados;
- 7.5.8.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;
- 7.5.8.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.
- 7.5.9. Quando houver glosa parcial dos serviços, a contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.
- 7.5.10. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 7.5.11. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 7.5.12. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da ANTT.
- 7.5.13. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da [Instrução Normativa nº 3, de 26 de abril de 2018](#).
- 7.5.14. Não havendo regularização ou sendo a defesa considerada improcedente, a ANTT deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 7.5.15. Persistindo a irregularidade, a ANTT deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 7.5.16. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 7.5.17. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da ANTT.
- 7.5.18. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da [Lei nº 8.212/1991](#), nos termos do item 6 do Anexo XI da [IN SEGES/MP nº 5/2017](#), quando couber.
- 7.5.19. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.
- 7.5.20. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela ANTT, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

EM = $I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	(6 / 100)	I = 0,00016438
		365	TX = Percentual da taxa anual = 6%

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. A contratação resta estimada em R\$ R\$ 1.668.282,00 (um milhão, seiscentos e sessenta e oito, duzentos e oitenta e dois mil reais), nos termos da tabela abaixo:

Item	Descrição	Métrica	Quantidade	CATSER	Valor Unitário Máximo Aceitável R\$	Valor Total Máximo Aceitável R\$
1	Subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.	Dispositivo	3.300	27456	505,54	1.668.282,00
VALOR TOTAL GLOBAL R\$						R\$ 1.668.282,00

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. A presente contratação correrá por conta dos recursos orçamentários constantes do Orçamento Geral da União, aprovado pela LOA - Lei Orçamentária Anual de 2022, da seguinte forma:

Gestão/Unidade	Programa de Trabalho	Natureza da despesa
39250/393001	26.126.0032.218T.0001	33.90.40

9.2. Os pagamentos serão efetuados obedecendo aos seguintes critérios:

Descrição	Periodicidade	Condições de Pagamento
Subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento.	Parcela Única	Mediante a entrega do objeto referente a cada Ordem de Serviço (OS) emitida, apresentação da Relação de licenças efetivamente instaladas/ativadas, apresentação do Termo de Recebimento Definitivo e a apresentação da NF

10. DA VIGÊNCIA DO CONTRATO

10.1. O contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos até o limite de 48 (quarenta e oito) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Art. 57, inciso IV, da Lei nº 8.666, de 1993.

10.2. A prorrogação do contrato dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada de a realização de pesquisa de mercado que demonstre a vantajosidade dos preços contratados para a Administração.

11. DO REAJUSTE DE PREÇOS

11.1. Os preços são fixos e irremovíveis no prazo de um ano contado da data limite para a apresentação das propostas.

11.2. Dentro do prazo de vigência do contrato, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o [Índice de Custo de Tecnologia da Informação \(ICTI\)](#), do Instituto de Pesquisa Econômica Aplicada (IPEA) exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

11.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

11.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.7. O reajuste será realizado por apostilamento.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Regime, Tipo e Modalidade da Licitação

12.1.1. O regime da execução do contrato ocorrerá por execução indireta através de empreitada por preço unitário, e o tipo e critério de julgamento da licitação é o menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

12.1.2. De acordo com o Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de Pregão, na forma eletrônica, com julgamento pelo critério de menor preço.

12.1.3. A fundamentação pauta-se na premissa que a contratação de serviços baseia-se em padrões de desempenho e qualidade objetivamente definidos no Termo de Referência, por meio de especificações reconhecidas e usuais do mercado, caracterizando-se como “serviço comum” conforme Inciso II, art. 3º, do Decreto nº 10.024, de 2019.

12.1.4. 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.

12.2. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.2.1. Nos termos da legislação vigente, quando aplicável, conforme previsão em EDITAL, nas aquisições de bens e serviços de informática e automação definidos pela Lei nº 8.248, de 1991, será assegurado o direito de preferência conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010, e nos art. 44 e 45 da Lei Complementar nº 123, de 14 de dezembro de 2006.

12.2.2. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

12.2.3. Destacando-se que a aplicação desse critério e direito ocorre de forma automática no sistema compras governamentais.

12.3. Critérios de Qualificação Técnica para a Habilitação

12.3.1. Independente do cumprimento das exigências relativas à Habilitação Jurídica, Econômico-Financeira e Fiscal, a CONTRATADA deverá:

12.3.1.1. Apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove aptidão para execução do objeto da contratação, com no mínimo, 50% (cinquenta por cento) do quantitativo do objeto da contratação, ou seja, 1.650 dispositivos, contendo as seguintes informações:

- Identificação do órgão ou empresa emitente com nome ou razão social, CNPJ, endereço completo, nome da pessoa responsável e função no órgão ou empresa, telefone e fax para contato;
- Indicação do CONTRATANTE de que foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);
- Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação, considerando;
- Data de emissão do atestado ou da certidão;
- Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto ao órgão ou empresa emitente).

12.3.2. Os atestados de capacidade técnica, a serem utilizados para comprovação dos serviços executados, deverão referir-se a um período mínimo de 12 (doze) meses.

12.3.3. Os atestados deverão ser válidos e conter a descrição pormenorizada dos softwares, bancos de dados, sistemas operacionais, arquitetura e demais componentes utilizados.

12.3.4. Ficará a cargo da ANTT, caso julgue necessário, realizar diligências para averiguação das informações constantes dos atestados de capacidade técnica apresentados.

12.3.5. No caso de atestados emitidos por pessoas jurídicas de direito privado, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa CONTRATADA.

12.3.6. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa licitante empresas controladas ou controladoras da empresa licitante ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa licitante.

12.3.7. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

12.3.8. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em foram prestados os serviços.

12.3.9. A licitante deverá apresentar Declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 8.666, de 1993.

13. SUBCONTRATAÇÃO E PARTICIPAÇÃO EM CONSÓRCIO

13.0.1. É vedada a subcontratação total ou parcial do objeto.

13.0.2. A vedação de que trata o item anterior, no caso da presente contratação, se deve ao fato de que não há como delimitar parcelas do objeto separadas do núcleo principal, constituído pelos itens que compõem o objeto. Sua execução deve estar sob a responsabilidade direta da CONTRATADA, de maneira a mitigar dificuldades em se delimitar responsabilidades em caso de descumprimento de cláusulas contratuais e níveis mínimos de serviço.

13.0.3. É vedada a participação de empresas em consórcio na licitação.

13.0.4. Não se vislumbra necessidade de permissão da participação em consórcio, tendo em vista o tamanho e a complexidade do objeto.

13.0.5. A vedação de empresas em consórcio não acarretará em restrição à competitividade, pois constatou-se a existência no mercado de diversas empresas prestadoras dos serviços objeto desta contratação, que encontram-se aptas a atender as exigências de habilitação previstas neste TERMO DE REFERÊNCIA, de modo que ao permitir a reunião de empresas em consórcio poderia estar restringindo a competitividade, ao possibilitar que empresas aptas à execução do objeto se reúnam e deixem de concorrer entre si.

14. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

14.1. A Equipe de Planejamento da Contratação foi instituída pelo Documento de Designação (SEI nº 12906220).

14.2. Conforme o §6º do art. 12 da IN SGD/ME nº 1, de 2019, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

<i>(Assinado eletronicamente)</i> JOÃO PROCÓPIO DO REGO NETO Integrante Requisitante	<i>(Assinado eletronicamente)</i> VICTOR HUGO GOUVEIA DE LUCENA LIMA Integrante Técnico	<i>(Assinado eletronicamente)</i> THIAGO REIS VICTORINO Integrante Administrativo
---	--	--

Aprovo,

Autoridade Máxima da Área de TIC
<i>(Assinado eletronicamente)</i> DIOGO DA FONSECA TABALIPA Superintendente de Tecnologia da Informação

APÊNDICES

Apêndice "A" - Requisitos Técnicos Mínimos da Solução

Apêndice "B" - Modelo de Proposta de Preços

Apêndice "C" - Modelo de Ordem de Serviço

Apêndice "D" - Modelo de Declaração de Sustentabilidade Ambiental

Apêndice "E" - Modelo de Declaração de Ciência e Consentimento da LGPD

Apêndice "F" - Termo de Recebimento Provisório

Apêndice "G" - Termo de Recebimento Definitivo

Apêndice "H" - Termo de Confidencialidade da Informação

Apêndice "I" - Termo de Ciência

Apêndice "J" - Termo de Encerramento do Contrato



Documento assinado eletronicamente por **JOÃO PROCÓPIO DO REGO NETO**, Integrante Requisitante, em 25/11/2022, às 16:26, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **VICTOR HUGO GOUVEIA DE LUCENA LIMA**, Integrante Técnico, em 25/11/2022, às 16:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **DIOGO DA FONSECA TABALIPA**, Superintendente, em 25/11/2022, às 18:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.antt.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **14325282** e o código CRC **88D5F2A6**.

APÊNDICE "A"**REQUISITOS MÍNIMOS DA SOLUÇÃO****1. DESCRIÇÃO DOS REQUISITOS MÍNIMOS DA SOLUÇÃO**

1.1. Contratação de serviço anual de subscrição de solução corporativa de proteção de dispositivos, contemplando instalação, configuração, suporte com operação assistida e transferência de conhecimento conforme tabela abaixo:

Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
1	Serviço anual de Subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimento.	Dispositivos	3.300		

2. DESCRIÇÃO DOS REQUISITOS TÉCNICOS OBRIGATÓRIOS

2.1. A console de administração deve ser centralizada para gerenciar todos os dispositivos, independentemente da localização geográfica.

2.2. A console de administração deve ser acessível em qualquer ponto da rede da contratante até mesmo quando estiverem conectados a redes públicas sem a necessidade de uma conexão VPN;

2.3. A solução deverá ser baseada em plataforma de nuvem e oferecida como serviço seguindo boas práticas.

2.4. A administração deve estar acessível através de HTTPS usando pelo menos um dos navegadores abaixo:

- a) Google Chrome;
- b) Edge;
- c) Firefox;

2.5. A administração da solução deverá ser 100% em nuvem sem a necessidade de instalação de ferramenta local para o gerenciamento da solução;

2.6. A gerência de administração da solução deve ter capacidade de separar os dispositivos gerenciados através de grupo via seleção manual e a criação de grupos com adição de dispositivos de forma automática com base em no mínimo, os critérios abaixo:

- a) Domínio;
- b) Endereços IP;
- c) Hostname parcial ou completo;
- d) Versão de sistema operacional;
- e) Unidade Organizacional do Active Directory;
- f) Versão do agente.

2.7. A gerência deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;

2.8. O uso de um fator de autenticação duplo deve ser utilizado para autenticação na console de gerenciamento da solução;

2.9. Deve ser possível a definição de papéis (RBAC) para os usuários dentro da console de administração delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;

2.10. A console de gerenciamento deve oferecer suporte Single Sign On com compatibilidade de pelo menos 3 opções distintas de provedor de identidade (IdP) na qual uma das opções deve ser obrigatoriamente Active Directory Federation Services (AD FS);

2.11. A console deve contemplar, no mínimo, as seguintes visualizações;

- a) Agentes ativos;
- b) Agentes por sistema operacional;
- c) Detecções por objetivo do ataque;
- d) Detecções por tática do ataque;
- e) Detecções por severidade do ataque.

2.12. A solução deverá suportar a instalação de agentes e/ou sensores diretamente no sistema operacional de cada máquina virtual ou diretamente no virtualizador

(hypervisor) sendo as duas formas aceitas;

2.13. A console de administração deve centralizar a administração dos sistemas operacionais Windows, Mac OS e Linux, não sendo aceitas múltiplas consoles para administração;

2.14. A console de gerência central deve ser capaz de atualizar os agentes de forma automática definida via política considerando no mínimo as seguintes opções;

- a) Versão mais recente;
- b) Versão específica;
- c) Uma versão anterior a mais recente (N-1);
- d) Duas versões anteriores a mais recente (N-2);

2.15. A plataforma deverá prevenir e remediar ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais.

2.16. A plataforma em nuvem deverá cumprir com as exigências da acreditação NSA-CIRA (certificando que foi avaliada e certificada em áreas de foco críticas derivadas das práticas recomendadas da indústria e do governo para investigação de segurança cibernética).

2.17. A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes).

2.18. A solução deve possuir um único software agente instalado em cada dispositivo para prover todas as funcionalidades descritas neste documento e que serão administradas através da conexão com a console de gerenciamento. Não será aceita a instalação de componentes adicionais como agentes de comunicação com múltiplos subagentes, plug-ins e softwares de terceiros para o atendimento dos requisitos;

2.19. O agente deve suportar os seguintes sistemas operacionais:

- a) Windows Server 2022;
- b) Windows Server 2019;
- c) Windows Server 2016;
- d) Windows Server 2012 R2;
- e) Windows Server 2012;
- f) Windows Server 2008 R2 SP1;
- g) Windows 11;
- h) Windows 10;
- i) Windows 8.1;
- j) Windows 7 SP1;
- k) Debian 9;
- l) Debian 10;
- m) SUSE Linux Enterprise (SLES) 11.4
- n) SUSE Linux Enterprise (SLES) 12.2 – 12.5
- o) SUSE Linux Enterprise (SLES) 15 – 15.3
- p) CentOS ou Red Hat Enterprise Linux (RHEL) 6.7 - 6.10
- q) CentOS ou Red Hat Enterprise Linux (RHEL) 7.4 - 7.7;
- r) CentOS ou Red Hat Enterprise Linux (RHEL) 8.0 - 8.5;
- s) Red Hat Enterprise Linux (RHEL) 8.6;
- t) Red Hat Enterprise Linux (RHEL) 9.0;
- u) Ubuntu 18.04 LTS;
- v) Ubuntu 20.04 LTS;
- w) Ubuntu 22.04 LTS.

2.20. A comunicação entre o agente e a console de gerenciamento deve utilizar um túnel de segurança TLS criptografado utilizando certificate pinning;

- a) A capacidade de *certificate pinning* implementada no agente não deverá permitir a relação de confiança com o armazenamento de chaves local do sistema operacional, ou seja, mesmo se um certificado raiz for adicionado na keystore local o agente não deverá herdar essa relação de confiança.

2.21. O agente deve suportar comunicação com a console de gerenciamento através de proxy.

2.22. Características específicas para sistemas operacionais Windows

- a) As seguintes opções de proxy deverão ser suportadas pelo agente, suportando no mínimo a combinação de duas ou mais opções ao mesmo tempo;
- b) Proxy configurado manualmente na estação ou via GPO;
- c) PAC configurado manualmente na estação ou via GPO;
- d) WPAD configurado para detectar automaticamente um arquivo PAC via DHCP ou DNS;
- e) Proxy definido no agente.

2.22.1. Quando o agente for configurado para utilizar 2 ou mais das configurações de proxy as mesmas devem ser acumulativas, ou seja, se for configurado proxy específico a nível de agente e o mesmo não estiver disponível ele deverá usar o proxy da estação e em último caso tentar a conexão direta;

2.22.2. Deverá ser possível configurar o agente para utilizar conexão direta, ou seja, ignorar qualquer configuração de proxy existente na máquina;

2.22.3. O agente deve implementar proteção de desinstalação através de token específica para cada dispositivo gerenciado.

2.22.4. Deve detectar tentativas de manipulação indevida dos componentes do agente;

2.22.5. Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

2.22.6. Não serão aceitas soluções que utilizem somente assinaturas para reconhecer ameaças;

2.22.7. O ML (Machine Learning) deve realizar a detecção e prevenção de artefatos maliciosos conhecidos e desconhecidos não somente na tentativa de execução, como também na tentativa de escrita do binário em disco, ou seja, se um binário considerado malicioso pelo motor de ML for escrito em disco deverá resultar em uma detecção e prevenção no momento da operação de escrita em disco.

2.22.8. Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.

2.22.9. Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

2.22.10. Deve ser capaz de detectar Adware e programas potencialmente indesejados;

- 2.22.11. Deve ser capaz de detectar ameaças mesmo que o dispositivo não esteja conectado à Internet;
- 2.22.12. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
- 2.22.13. Deve permitir bloqueio de scripts e comandos em Powershell considerados suspeitos;
- 2.22.14. Deve permitir bloqueio automático de processos suspeitos;
- 2.22.15. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;
- 2.22.16. Deve permitir bloqueio de operações em registros suspeitos;
- 2.22.17. Deve permitir que arquivos maliciosos possam ser movidos para uma área de quarentena;
- 2.22.18. Deve possuir integração com o Windows Security Center para ser reconhecido como uma solução de proteção válida para antimalware;
- 2.22.19. Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória;
- 2.22.20. Deve ser capaz de forçar Data Execution Prevention de forma a impedir ataques que utilizem espaço de memória para execução de códigos em região de memória não executável;
- 2.22.21. Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;
- 2.22.22. Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);
- 2.22.23. Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos;
- 2.22.24. Deve ser capaz de detectar malwares do tipo Ransomware com base em, no mínimo, os comportamentos abaixo:
 - a) Deletar backups;
 - b) Operações em excesso ao sistema de arquivos;
 - c) Criptografia de arquivos;
 - d) Processos associados a malwares de ransomware Cryptowall, Wannacry, Locky;
 - e) Processo suspeito de deleção de um volume de “Shadow Copies”

2.22.25. Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos:

2.22.26. Criação de processos suspeitos originados de navegadores;

2.22.27. Detecção de comprometimento de servidores Web através de webshell;

2.22.28. Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;

2.22.29. Injeção de código não esperada de um processo a outro;

2.22.30. Execução de JavaScript através do executável Rundll32.

2.22.31. Deve ser capaz de detectar movimentação lateral através de circunvenção do processo de logon do Windows;

2.22.32. Deve ser capaz de detectar de processos que tentam obter credenciais de login;

2.22.33. A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK;

a) T1003, T1012, T1018, T1021, T1026, T1027, T1036, T1047, T1048, T1049, T1053, T1055, T1059, T1061, T1070, T1087, T1095, T1102, T1110, T1112, T1132, T1133, T1136, T1204, T1218, T1219, T1222, T1482, T1486, T1489, T1490, T1505, T1529, T1543, T1547, T1548, T1550, T1056, T1558, T1559, T1560, T1562, T1564, T1567, T1570, T1571, T1574.

2.22.34. O agente para estações Windows deve suportar a RFC 5246;

2.22.35. Deve permitir que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no dispositivo gerenciado;

2.22.36. Deve permitir exclusão de arquivos e pastas utilizando caracteres coringa (Wildcard);

2.22.37. Deve permitir rodar comandos no dispositivo em tempo real por meio da console de gerenciamento em nuvem, precisando contemplar as seguintes ações:

a) Mostrar as conexões de rede

b) Mostrar os processos ativos

c) Encerrar um processo ativo

d) Reiniciar o dispositivo

- e) Desligar o dispositivo
- f) Acessar e deletar arquivos
- g) Iniciar execução de um processo;
- h) Dump de memória do dispositivo;

2.22.38. Deve permitir a definição granular da execução ou não de, no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no dispositivo via console de gerenciamento;

- a) Extração de arquivos;
- b) Iniciar execução de um processo;
- c) Dump de memória do dispositivo;

2.22.39. Deve permitir que scripts Powershell possam ser adicionados à solução para que possam ser executados remotamente em resposta à um incidente de segurança;

2.22.40. Deve permitir que o acesso remoto seja desabilitado globalmente em dispositivos específicos;

2.22.41. Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;

2.22.42. Deve permitir que administradores possam interromper tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento;

2.22.43. Possuir a capacidade de adição de endereços específicos para mesmo quando o dispositivo esteja em quarentena/contenção sejam alcançáveis, ou seja, quando houver o isolamento do dispositivo o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a console de gerência;

2.22.44. Deve permitir que proteção de dispositivos seja habilitada em modos de detecção somente, sem bloqueio efetivo;

2.22.45. Deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivo.

- a) Dispositivos de imagem;
- b) Dispositivos de áudio e vídeo;
- c) Dispositivos de armazenamento em massa;
- d) Dispositivos móveis (MTP/PTP);

- e) Impressoras;
- f) Adaptadores de rede wireless;
- g) Para dispositivos de armazenamento em massa, deve permitir acesso granular com no mínimo, as seguintes permissões:

- Leitura somente;
- Escrita e leitura;
- Escrita leitura e execução;
- Bloqueio total;

2.22.46. A proteção de dispositivos deve permitir exceções baseadas no Vendor ID e Product ID, número serial e classe;

2.22.47. Administração Firewall Local na mesma console;

- a) Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;
- b) A política de firewall deve permitir a utilização de múltiplas regras de firewall;
- c) As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;
- d) Regras de firewall devem suportar minimamente as seguintes características:
 - IPv4;
 - IPv6;
 - Protocolos:
 - Any;
 - TCP;
 - UDP;
 - ICMP;
 - Avançado (permitindo especificar o número do protocolo).
 - Endereço local;
 - Porta local;
 - Endereço remoto;
 - Porta remota;
 - Ação:
 - Permitir;

- Bloquear.
 - Direção da conexão:
 - Inbound;
 - Outbound;
 - Inbound ou Outbound.
- e) Perfil de rede (para que a regra seja aplicada de acordo com o perfil da interface de rede):
- Domínio;
 - Privado;
 - Público.
 - Processo;
- f) Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;
- g) As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente.

2.23. Características específicas para sistemas operacionais Linux

- a) Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção de ataques;
- b) Deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;
- c) Deve permitir níveis de sensibilidade diferentes para detecção de ataques através do componente de aprendizado de máquina;
- d) Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
- e) Deve permitir bloqueio de processos com comportamento malicioso de acordo com a inteligência da fabricante.
- f) Deve permitir rodar comandos no dispositivo em tempo real por meio da console de gerenciamento em nuvem, precisando contemplar as seguintes ações:
- Mostrar as conexões de rede

- Mostrar os processos ativos
 - Encerrar um processo ativo
 - Reiniciar o dispositivo
 - Desligar o dispositivo
 - Acessar e deletar arquivos
- g) Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;
- h) Deve permitir que administradores possam interromper tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento.
- i) Possuir a capacidade de adição de endereços específicos para mesmo quando o dispositivo esteja em quarentena/contenção sejam alcançáveis, ou seja, quando houver o isolamento do dispositivo o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a console de gerência.
- j) Deve permitir monitorar atividade de arquivos de sistema para enriquecer a telemetria enviada a nuvem, melhorando a qualidade das detecções.
- k) Deve permitir monitorar atividade de rede para enriquecer a telemetria enviada a nuvem, melhorando a qualidade das detecções.

2.24. Capacidades de inteligência de ameaças

2.24.1. A inteligência de ameaças deve mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, país de origem da campanha e última atividade;

2.24.2. Para campanhas de ameaça, a inteligência de ameaças deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de entrega, breve descrição da campanha, forma de monetização, métodos de ataque e motivação da campanha.

2.24.3. Deve associar, quando pertinente, detecções presentes no ambiente à campanha de ataque;

2.24.4. Deve permitir extração de indicadores de comprometimento como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de email, nomes de arquivos associados às atividades maliciosas;

2.25. Capacidades de emulação de execução de código

2.25.1. A solução deve prover, integrada à console de administração, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros;

2.25.2. Deve se integrar ao agente instalado em dispositivos para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;

2.25.3. A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais:

- a) Windows 7 (32 e 64 bits);
- b) Windows 10;
- c) Linux Ubuntu;
- d) Android.

2.25.4. A solução deve incluir na análise de execução, no mínimo, as seguintes características:

- a) Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK;
- b) Características comportamentais suspeitas;
- c) Imagens de execução, quando aplicável;
- d) Detalhes do arquivo como nome, hash, tamanho, tipo;
- e) Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
- f) Atividades de arquivos;
- g) Detalhes de processos iniciados durante a execução.

2.26. Relatórios e dashboard.

2.26.1. A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.

2.26.2. A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada, como por exemplo por tática.

2.26.3. A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.

2.26.4. A plataforma deverá ter a capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros:

- a) Severidade;
- b) Tática;
- c) Técnica;
- d) Usuário;
- e) Host
- f) Tipo de sistema operacional;
- g) Versão do sistema operacional;
- h) Última hora;
- i) Último dia;
- j) Última semana;
- k) Últimos 30 dias
- l) Nome de arquivo;
- m) Hash do processo

2.26.5. A solução deve prover a capacidade de relatório de todas as conexões remotas realizadas desde a console de gerenciamento ao endpoint gerenciado contendo minimamente as seguintes informações que não deverão ser passíveis de exclusão ou limpeza, garantindo assim o não-repúdio:

- a) Login do administrador/operador que realizou a operação;
- b) Nome do endpoint.
- c) Duração da sessão.
- d) Data e hora do início da sessão;
- e) Arquivos copiados desde a máquina;
- f) Comandos executados na máquina;
- g) Data e hora de cada comando executado.

2.26.6. A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV:

- a) Hostname;
- b) Data e hora da primeira comunicação.
- c) Data e hora da última comunicação.
- d) Versão do sistema operacional;
- e) Modelo;
- f) Tipo;

- g) Unidade organizacional (OU);
- h) Site;
- i) Política de proteção aplicada;
- j) Política de resposta aplicada;
- k) Política de atualização aplicada;
- l) Política de controle de dispositivos USB aplicada;
- m) Identificação do host (UID/GUID);
- n) IP local da máquina;
- o) IP público da máquina;
- p) MAC Address;
- q) Versão do sensor/agente instalado.

2.26.7. O relatório de máquinas deverá ter a capacidade de aplicar filtros para inclusão ou exclusão de dados no relatório, considerando minimamente as seguintes opções de filtro:

- a) Domínio;
- b) Grupo;
- c) Identificação do host (UID/GUID);
- d) Hostname;
- e) IP local da máquina;
- f) MAC Address;
- g) Subnet da máquina;
- h) Versão do sistema operacional;
- i) Unidade organizacional (OU);
- j) Plataforma;
- k) Política de proteção aplicada;
- l) Política de resposta aplicada;
- m) Política de atualização aplicada;
- n) Versão do sensor/agente instalado.

2.26.8. Deverá apresentar a lista de dispositivos gerenciados com a capacidade de filtro baseado minimamente nas seguintes categorias;

- a) Por tipo do Sistema Operacional;
- b) Por versão do Sistema Operacional;

- c) Por plataforma do Sistema Operacional;
- d) Por unidade organizacional do host;
- e) Por nome do Site;
- f) Por Status do host;

2.27. Workflows e notificações

2.27.1. A solução deve possibilitar a criação de workflows de automatização para definir ações que o administrador quer que a solução execute em resposta a uma detecção, a uma política e uma atualização feita por um usuário.

2.27.2. Deve permitir a configuração dos seguintes gatilhos de início do workflow:

- a) Nova detecção
- b) Detecção atribuída a um usuário para investigação
- c) Política criada
- d) Política deletada
- e) Política habilitada
- f) Política desabilitada;
- g) Política atualizada.

2.27.3. Deve permitir a configuração das seguintes ações tomadas automaticamente

- a) Conter a rede do dispositivo, fazendo que ele só se comunique com a console da solução
- b) Pegue o arquivo associado a uma detecção da endpoint e faça o upload para a console
- c) Remova o arquivo associado a uma detecção do endpoint
- d) Notifique um usuário

2.27.4. A solução deve possibilitar a configuração dos seguintes canais de notificação no workflow:

- a) E-mail
- b) Microsoft Teams
- c) PagerDuty
- d) ServiceNow
- e) Slack
- f) Webhook

2.27.5. A solução deve possibilitar a configuração dos seguintes canais de notificação

no workflow:

- a) E-mail
- b) Microsoft Teams
- c) PagerDuty
- d) ServiceNow
- e) Slack
- f) Webhook

2. IMPLANTAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

2.1. Durante a etapa de implantação e migração, a solução fornecida pela CONTRATADA deverá ser colocada em plena operação, em condições reais de produção, e sua equipe deverá estar presente, nos horários de testes, implantação e migração, definidos pela ANTT, e estes horários poderão ser horário comercial, período noturno ou final de semana.

2.2. Compreende-se nesta etapa a instalação e configuração da solução e integração com os dispositivos necessários a serem protegidos, que deverá ser realizada em no máximo 15 (quinze) dias contados da data de assinatura do Contrato.

2.3. Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários e acessos necessários de acordo com as políticas e diretrizes de segurança da agência.

2.4. As atividades de instalação e configuração inicial da solução, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da ANTT.

2.5. A solução deverá ser instalada e configurada a integração com os dispositivos necessários a serem protegidos, em no máximo 15 (quinze) dias contados da data de assinatura do Contrato, e durante esta etapa, a equipe da CONTRATADA deverá estar de forma remota, nos horários de instalação definidos pela ANTT e nos casos de atuações remotas, deverá pré-agendar com a equipe da ANTT os horários necessários para os acessos necessários de acordo com as políticas e diretrizes de segurança da ANTT, sendo que as atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou finais de semana, de acordo com a definição da equipe da ANTT e para esta ou qualquer outra

etapa a ANTT não disponibilizará qualquer infraestrutura de hardware e/ou software, apenas parte da equipe acompanhará a ativação dos serviços, da console e a integração com os dispositivos, mantendo o alinhamento com ato PGJ 939/2019 da ANTT visando a transformação digital e seguindo a diretriz de fazer mais, melhor e com menos estrutura local.

3. DO SUPORTE TÉCNICO COM OPERAÇÃO ASSISTIDA E TRANSFERÊNCIA DE CONHECIMENTO

3.1. Os atendimentos deverão ser do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, e deverá ser realizado por profissionais especializados, sendo necessário cobrir todo e qualquer defeito ou demanda apresentada.

3.1.1. Os serviços de suporte e manutenção consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e atualizações de versões para correções de eventuais problemas identificados.

3.1.2. As atividades de suporte técnico serão realizadas, a critério da ANTT, em seu ambiente, a partir da assinatura do Contrato e durante toda sua vigência contratual.

3.1.3. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração com os dispositivos da ANTT, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

3.1.3.1. Orientação sobre acesso, o uso, a configuração, a instalação da solução e a integração com os dispositivos da ANTT, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do FABRICANTE da solução.

3.1.3.2. Orientação quanto às melhores práticas para implementação e integração da solução no ambiente da ANTT.

3.1.3.3. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu impacto nos agentes e/ou sensores já instalados no ambiente da ANTT.

3.1.3.4. Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas nos dispositivos protegidos e monitorados pela console central.

3.1.3.5. Aplicação de melhores práticas para implementação dos produtos de software adquiridos.

3.1.3.6. Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam.

3.1.3.7. Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas.

3.1.3.8. Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias novas integrações.

3.1.3.9. Identificação de melhorias e respectivo tratamento (melhoria de parametrização).

3.1.3.10. Parametrização da solução, de acordo com as regras e políticas disponíveis em sua console única e definidas pela ANTT.

3.1.3.11. Apoio para execução de procedimentos de atualização para novas versões dos agentes e/ou sensores instalados nos dispositivos

3.1.3.12. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário.

3.1.3.13. Suporte avançado para estratégia e planejamento de migrações e adequações nos agentes e sensores instalados nos dispositivos protegidos pela solução.

3.1.3.14. Avaliação e comparação de novas funcionalidades de forma remota e se necessário presencial, mediante solicitação prévia da equipe da ANTT.

3.1.3.15. Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

3.1.3.16. A ANTT poderá solicitar durante toda a vigência contratual do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe, para isso serão abertos chamados com severidade "4"

classificado como “baixa”.

3.1.3.17. As transferências de conhecimento poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverá ser realizado nas dependências da ANTT, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da ANTT, de modo que os alunos possam absorver os conhecimentos oficiais do fabricante acerca da solução fornecida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

3.1.3.18. Serão solicitadas no mínimo, 2 (duas) workshops de transferência de conhecimento, sendo uma na implantação da solução, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente na ANTT e no máximo 1 (uma) workshop de transferência de conhecimento por mês caso a equipe da ANTT entenda que seja necessário.

3.1.3.19. Para os casos em que houver alguma mudança significativa que reflita na operação da solução ou reflita nos agentes e/ou sensores instalados nos dispositivos, a CONTRATADA deverá transferir este conhecimento para equipe interna da ANTT sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4”.

3.1.3.20. Os serviços de operação assistida poderão ser de forma remota ou se for exigido como ação necessária e primordial, deverão ser realizados nas dependências da ANTT, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da SETUR, de modo que os trabalhos possam ser realizados com qualidade e eficácia, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe da ANTT, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.

3.1.3.21. Será solicitado no mínimo, 1 (uma) sessão de operação assistida por trimestre, e no máximo 1 (uma) sessão por mês, devendo ocorrer logo após a implantação da solução, para possibilitar qualquer nova análise de funcionamento, configuração e/ou modificação necessárias nas implementações e integrações já realizadas, de modo que o funcionamento se mantenha sempre atualizado, em produção e devidamente funcional e integrado aos dispositivos pertencentes ao ambiente da ANTT.

3.1.4. O serviço deverá ocorrer durante toda a vigência contratual, e deverá ser disponibilizado pela CONTRATADA um sistema de acompanhamento e controle de chamados onde eles serão registrados com acesso liberado para cada integrante da equipe da ANTT que será informado no início da vigência contratual.

3.1.4.1. O sistema deverá permitir abertura de chamados via telefone, e-mail e/ou console de acesso web pela equipe da ANTT.

3.1.4.2. Em casos de chamados abertos via telefone, o sistema deverá disponibilizar um número local onde a ANTT possui sua sede (Brasília, evitando custos desnecessários, onde o número deverá ser disponibilizado pela CONTRATADA no formato (061)+(número local) e deverá possibilitar a abertura de chamados por meio de gravação de áudio, caso os atendentes estejam ocupados no momento da ligação, devendo o sistema identificar o número utilizado pré-cadastrado e liberado para abertura de chamados que serão automaticamente abertos e enviados para uma fila de atendimentos apropriada, devendo registrar o horário do momento da ligação como horário de abertura do chamado em questão.

3.1.5. Os serviços serão prestados de forma remota observando as seguintes condições:

3.1.5.1. O suporte poderá ser prestado por telefone, e-mail, chat ou internet, prioritariamente serão abertos os chamados via e-mail.

3.1.5.2. Durante as sessões remotas a CONTRATADA deverá utilizar ferramenta própria para acesso remoto seguro (exemplo: Bomgar, LogMeIn) ao ambiente da ANTT, possibilitando a gravação da sessão e possibilitando o acesso simultâneo de todos os envolvidos na solução do chamado, seguindo todas as diretrizes de segurança pré-estabelecidas.

3.1.5.3. Para chamados de severidade Crítica, Alta, Normal ou Baixa, o início dos atendimentos realizados e os prazos de solução estão especificados na tabela a seguir:

Severidade	Descrição	Prazo máximo de início de atendimento remoto	Prazo máximo da solução
Urgente / Crítica Severidade 1	Situação emergencial ou problema crítico que cause indisponibilidade do ambiente.	Até 2 (duas) horas após a abertura do chamado remoto.	Até 72 (setenta e duas) horas após abertura do chamado remoto.
Alta Severidade 2	Impacto de alta significância relacionado à utilização do ambiente: ocorrência de indisponibilidade de funcionalidade ou recurso importante onde as operações continuam de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Até 4 (quatro) horas após a abertura do chamado remoto.	Até 5 (cinco) dias após abertura do chamado remoto.
Normal Severidade 3	Impacto de baixa significância relacionado à utilização do ambiente. Não há ocorrência de indisponibilidade de funcionalidade ou recurso, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 (oito) horas após a abertura do chamado remoto.	Até 8 (oito) dias após abertura do chamado remoto.
Baixa Severidade 4	Consulta e/ou dúvida técnica e/ou transferência de conhecimento	Até 24 (vinte e quatro) horas após a abertura do chamado remoto.	Até 10 (dez) dias após a abertura do chamado remoto.

3.1.6. Não haverá limite para o número de chamados de suporte técnico.

3.1.7. O nível de severidade será atribuído pela equipe autorizada da ANTT no momento da abertura do chamado.

3.1.8. Durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que a ANTT estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de

protocolo/número de abertura do mesmo.

3.1.9. Uma vez que a solução estará em produção e funcionando em nuvem, as atividades relacionadas a correções ou atualizações da console que necessitarem indisponibilidade do ambiente, sem prejuízo para o funcionamento dos dispositivos já gerenciados pela solução, deverão ser notificadas a ANTT com antecedência mínima de 1 (um) dia útil.

3.1.10. O descumprimento dos prazos de nível de serviço de atendimento implicará na aplicação de advertências formais e caso seja definido pela ANTT poderão ser aplicadas glosas conforme tabela a seguir e serem descontadas da garantia financeira dos serviços prestados:

Resultado esperado e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
Crítica	1hora	$NHA * 0,7\% * VAS$	10% da VAS
Alta	1hora	$NHA * 0,5\% * VAS$	10% da VAS
Média	1hora	$NHA * 0,3\% * VAS$	10% da VAS

Onde:

NHA = Número de horas de atraso após o término do prazo máximo esperado para solução.

VAS = Valor anual da subscrição.

3.1.11. Durante o período de vigência do contrato a CONTRATADA deverá apresentar mensalmente relatório em formato eletrônico, contendo todos os chamados ocorridos no mês e seus prazos de atendimento, contendo informações analíticas e sintéticas de cada chamado, contendo a lista e total de chamados concluídos dentro e fora do prazo de SLA estabelecido.

3.1.12. Deverá ser garantido a ANTT pleno acesso as últimas atualizações e informações do FABRICANTE da solução, além de acesso irrestrito a solução, sendo obrigação da CONTRATADA a abertura de qualquer chamado necessário junto a equipe de suporte do FABRICANTE, caso seja necessário, devendo possuir todos os acessos necessários para a execução dos serviços de suporte técnico com a operação assistida e transferência de conhecimento.

----- FIM DO APÊNDICE "A" -----

APÊNDICE “B”**MODELO****PROPOSTA DE PREÇOS**

(em papel timbrado da empresa)

À**AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES****Superintendência de Gestão – SUDEG / Gerência de Licitações e Contratos - GELIC****Setor de Clubes Esportivos Sul – SCES, lote 10, trecho 03, Projeto Orla Polo 8****70200-003 - Brasília, DF****Referência:** Pregão Eletrônico nº ____/____.

Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual contratação de pelo sistema de registro de preços, de fornecimento de solução de gerenciamento de acesso lógico privilegiado, contemplando garantia de atualização de versões e serviços correlatos, para atender às necessidades da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, de acordo com as especificações e condições constantes do Pregão em referência, bem como do respectivo Edital e seus Anexos.

PLANILHA DE PROPOSTA DE PREÇOS

Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor Total
1	Serviço anual de Subscrição de solução de proteção de dispositivos com garantia de atualização de versões incluindo instalação e configuração e suporte técnico com operação assistida e transferência de conhecimento.	Dispositivos	3.300		

1) Dados da Proposta:Valor Total: R\$ _____ (**VALOR POR EXTENSO**).**2) Validade da Proposta:** 60 (sessenta) dias, a contar da data de sua apresentação.

3) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

4) Dados da empresa:

a) Razão Social: _____

b) CNPJ (MF) nº _____

c) Inscrição Estadual nº: _____

d) Endereço: _____

e) Telefone: _____ Fax: _____ e-mail: _____

f) Cidade: _____ Estado: _____

g) CEP: _____

h) Representante(s) legal(is) com poderes para assinar o contrato:

a. Nome: _____

b. Cargo: _____

c. CPF: _____ RG: _____ - _____

i) Dados Bancários:

a. Banco: _____

b. Agência: _____

c. Conta Corrente: _____

j) Dados para Contato:

a. Nome: _____

b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo “___” do Edital.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência.

Declaramos que, no valor acima apresentado, estão contidas todas as despesas, de quaisquer naturezas, que se fizerem indispensáveis à perfeita execução do objeto do termo de referência, bem como os custos operacionais, ou seja, àqueles diretamente relacionados à execução do contrato.

Declaramos, ainda, que inexistente qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidor ou dirigente da Agência Nacional de Transportes Terrestres; e que foi (realizada a Vistoria nas instalações da ANTT, tomando conhecimento dos serviços a serem realizados / apresentada recusa formal de Vistoria), não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

Local e data

Representante Legal
(com carimbo da empresa)
Cargo
CPF

----- FIM DO APÊNDICE "B" -----

APÊNDICE "C"

ORDEM DE SERVIÇO (OS) Nº

MODELO

CLIENTE			
PRESTADORA DE SERVIÇOS			
CONTRATO		VIGÊNCIA	
FISCAL DO CONTRATO			
E-MAIL		TELEFONE	
IDENTIFICAÇÃO/DIRECIONAMENTO			
SISTEMAS			
VOLUME ESTIMADO DOS SERVIÇOS			
Título - Assunto			
Descrição			
Origem/Solicitante			
Classificação			
Data de Abertura da OS			
Data estimada da Entrega			
Normas e Sigilo: De acordo com as normas e procedimentos da ANTT, segundo cláusula sétima do Contrato Administrativo.		Instruções: Deverão ser observados os procedimentos definidos pela SUTEC	
<p>Data: ____/____/____</p> <p>_____</p> <p style="text-align: center;">(nome) Gestor do Contrato</p> <p>_____</p> <p style="text-align: center;">(nome) Preposto</p>			

-----FIM DO APÊNDICE "C"-----

APÊNDICE "D"**MODELO****DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL**
(em papel timbrado da empresa)

Empresa		
CNPJ		Inscrição Estadual
Endereço		
Cidade		Estado
CEP	Telefone	E-mail institucional
Representante Legal		

DECLARO, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico **SRP** nº ____/____, instaurado pelo Processo nº _____, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da [Instrução Normativa SLTI/MP nº 1/2010](#).

Por ser a expressão da verdade, firmamos a presente.

Cidade/UF, ____ de _____ de ____.

Carimbo e Assinatura do Responsável/Representante da Empresa
(Nome legível)
CPF nº

-----FIM DO APÊNDICE "D"-----

APÊNDICE “E”**MODELO****DECLARAÇÃO DE CIÊNCIA E CONSENTIMENTO QUANTO AO CUMPRIMENTO DA LEI
GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018**

Processo Administrativo nº		Nº do Contrato	Data de Assinatura
Objeto			
Identificação da Empresa Contratada			
Nome da Empresa			
CNPJ		Inscrição Estadual	
Endereço			
Cidade		Estado	
CEP	Telefone	E-mail institucional	

por meio de seu representante legal, _____, portador da Carteira de Identidade nº _____, expedida pela ____, e inscrito no CPF sob o nº _____, DECLARA QUE:

1. Os eventuais dados pessoais relacionados à LICITANTE/CONTRATADA disponibilizados à ANTT para efeito de participação no presente certame e que possam ser exigidos para a execução contratual, serão tratados para finalidade específica, em conformidade com os termos do artigo 7º da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

3. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.

4. As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individuais ou coletivos aos titulares de dados pessoais repassados em decorrência da participação no certame e eventual execução contratual, por inobservância à LGPD.

Cidade/UF, ____ de _____ de ____.

(Nome do Diretor ou representante legal da empresa)

(Cargo)

(RG e CPF)

(Endereço)

(Endereço eletrônico e telefone)

----- FIM DO APÊNDICE “E” -----

APÊNDICE "F"

TERMO DE RECEBIMENTO PROVISÓRIO

MODELO

IDENTIFICAÇÃO			
Contrato:		Número da O.S.:	
Contratante:			
Contratada:			
Processo:		Pregão:	
Solução de TI:			

ESPECIFICAÇÃO DOS SERVIÇOS E VOLUME DE EXECUÇÃO					
Item	Descrição dos serviços	Métrica	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
1					
2					
Valor Global					

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso I, da Instrução Normativa nº 01 do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, de 04 de abril de 2019, que os serviços integrantes da O.S. acima identificada e/ou conforme definido no Modelo de Execução do contrato supracitado, foram executados no período de <data de início> a <data de finalização> e recebidos provisoriamente em <data do recebimento provisório>. Tais serviços serão objeto de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato pela Contratante.

Para fins de recebimento destes serviços foram entregues os seguintes documentos:

1) _____;

2) _____.

Ressaltamos que o recebimento definitivo destes serviços ocorrerá em até 07 (sete) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência, correspondente ao Contrato supracitado.

(nome)

Fiscal Técnico

Matrícula SIAPE: _____

Brasília/DF, ____/____/____.

-----FIM DO APÊNDICE "F"-----

APÊNDICE "G"**MODELO****TERMO DE RECEBIMENTO DEFINITIVO**

IDENTIFICAÇÃO			
Contrato:		Número da O.S.:	
Contratante:			
Contratada:			
Processo:		Pregão:	
Solução de TI:			

ESPECIFICAÇÃO DOS SERVIÇOS E VOLUME DE EXECUÇÃO					
Item	Descrição dos serviços	Métrica	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
1					
2					
Valor Global					

Por este instrumento, atestamos para fins de cumprimento do disposto no art. 33, inciso VIII, da Instrução Normativa nº 01 do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital, de 04 de abril de 2019, que os serviços integrantes da O.S acima identificada e/ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos definitivamente em <data do recebimento definitivo>, atendem às exigências especificadas no Termo de Referência do Contrato, com base no Relatório Circunstanciado elaborado pela fiscalização técnica e documentação apresentada.

(nome)

Fiscal Requisitante

Matrícula SIAPE: _____

Brasília/DF, ____/____/____.

(nome)

Fiscal Técnico

Matrícula SIAPE: _____

Brasília/DF, ____/____/____.

-----FIM DO APÊNDICE “G”-----

MODELOAPÊNDICE "H"**TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**

Processo Administrativo nº	Nº do Contrato	Data de Assinatura
Objeto		

A **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, com sede em Brasília-DF, inscrito no CNPJ sob o nº **04.898.488/0001-77**, doravante denominado **CONTRATANTE** e a **Empresa** _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada simplesmente **CONTRATADA**, representada neste ato pelo Sr _____, (cargo) _____, (nacionalidade) _____, (estado civil) _____, (profissão) _____, portador da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado em _____, e, sempre que em conjunto referidas como PARTES para efeitos deste **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, doravante denominado simplesmente TERMO, e,

CONSIDERANDO que, em razão do atendimento à exigência do Contrato nº ____/____, celebrado pelas PARTES, doravante denominado **CONTRATO**, cujo objeto é a **<objeto do contrato>**, mediante condições estabelecidas pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**;

CONSIDERANDO que o presente **TERMO** vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de **INFORMAÇÕES**, que a **CONTRATADA** tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES** de que a **CONTRATADA** tomar conhecimento em razão da execução do **CONTRATO**, respeitando todos os critérios estabelecidos aplicáveis às **INFORMAÇÕES**;

A **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES** estabelece o presente **TERMO** mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste **TERMO** é prover a necessária e adequada **PROTEÇÃO ÀS INFORMAÇÕES** da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, principalmente aquelas classificadas como **CONFIDENCIAIS**, em razão da execução do **CONTRATO** celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Parágrafo Primeiro: As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer **INFORMAÇÕES** reveladas pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Segundo: A **CONTRATADA** se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer **INFORMAÇÕES** que venham a ser fornecidas pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, a partir da data de assinatura deste **TERMO**, devendo ser tratadas como **INFORMAÇÕES CONFIDENCIAIS**, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Terceiro: A **CONTRATADA** se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das **INFORMAÇÕES** da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Quarto: A **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, com base nos princípios instituídos na Segurança da Informação, zelará para que as **INFORMAÇÕES** que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela **CONTRATADA**.

CLÁUSULA TERCEIRA - DAS LIMITAÇÕES DA CONFIDENCIALIDADE

Parágrafo Único: As obrigações constantes deste **TERMO** não serão aplicadas às **INFORMAÇÕES** que:

- I. Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;
- II. Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente **TERMO**;
- III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES ADICIONAIS

Parágrafo Primeiro: A **CONTRATADA** se compromete a utilizar as **INFORMAÇÕES** reveladas exclusivamente para os propósitos da execução do **CONTRATO**.

Parágrafo Segundo: A **CONTRATADA** se compromete a não efetuar qualquer cópia das **INFORMAÇÕES** sem o consentimento prévio e expresso da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

- I. O consentimento mencionado no Parágrafo segundo, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES.

Parágrafo Terceiro: A **CONTRATADA** se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste **TERMO** e da natureza confidencial das **INFORMAÇÕES** da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Quarto: A **CONTRATADA** deve tomar todas as medidas necessárias à proteção das **INFORMAÇÕES** da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Quinto: Cada PARTE permanecerá como única proprietária de todas e quaisquer **INFORMAÇÕES** eventualmente reveladas à outra parte em função da execução do **CONTRATO**.

Parágrafo Sexto: O presente **TERMO** não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

I. Os produtos gerados na execução do **CONTRATO**, bem como as **INFORMAÇÕES** repassadas à **CONTRATADA**, são única e exclusiva propriedade intelectual da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Sétimo: A **CONTRATADA** firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao **CONTRATO**, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

Parágrafo Oitavo: A **CONTRATADA** obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às **INFORMAÇÕES** que venham a ser reveladas durante a execução do **CONTRATO**.

CLÁUSULA QUINTA - DO RETORNO DE INFORMAÇÕES

Parágrafo Único: Todas as **INFORMAÇÕES** reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

I. A **CONTRATADA** deverá devolver, íntegros e integralmente, todos os documentos a ela fornecida, inclusive as cópias porventura necessárias, na data estipulada pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES** para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias.

II. A **CONTRATADA** deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da **AGÊNCIA NACIONAL DE TRANSPORTES**

TERRESTRES, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

CLÁUSULA SEXTA - DA VIGÊNCIA

Parágrafo Único: O presente **TERMO** tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do Contrato.

CLÁUSULA SÉTIMA - DAS PENALIDADES

Parágrafo Único: A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na **RESCISÃO DO CONTRATO** firmado entre as PARTES. Neste caso, a **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº 8.666/1993.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

Parágrafo Primeiro: Este **TERMO** constitui vínculo indissociável ao **CONTRATO**, que é parte independente e regulatória deste instrumento.

Parágrafo Segundo: O presente **TERMO** constitui acordo entre as PARTES, relativamente ao tratamento de **INFORMAÇÕES**, principalmente as **CONFIDENCIAIS**, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente.

Parágrafo Terceiro: Surgindo divergências quanto à interpretação do pactuado neste **TERMO** ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os

princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as **INFORMAÇÕES** da **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES**.

Parágrafo Quarto: O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à **CONFIDENCIALIDADE DE INFORMAÇÕES**.

Parágrafo Quinto: A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

Parágrafo Único: Fica eleito o foro da Justiça Federal - Seção Judiciária do Distrito Federal, em Brasília-DF, para dirimir quaisquer dúvidas oriundas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, a **CONTRATADA** assina o presente **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, em 2 (duas) vias de igual teor e um só efeito, na presença de duas testemunhas.

Cidade/UF, ____ de _____ de ____.

Nome do Diretor ou representante legal da empresa

Cargo

CPF nº

Gestor do Contrato

Matrícula

<<Cargo/Função>>

<<Setor/Departamento>>

Fiscal Técnico do Contrato

Matrícula

<<Cargo/Função>>

<<Setor/Departamento>>

-----FIM DO APÊNDICE "H"-----

MODELOAPÊNDICE "I"**TERMO DE CIÊNCIA**

Processo Administrativo nº	Nº do Contrato	Data de Assinatura
Objeto		
Identificação da Empresa Contratada		
Nome da Empresa		
CNPJ	Inscrição Estadual	
Endereço		
Cidade	Estado	
CEP	Telefone	E-mail institucional

Pelo presente instrumento, eu _____, CPF nº _____, RG nº _____, expedida em _____, órgão expedidor ____/____, prestador de serviço, ocupando o cargo de _____ na empresa _____, que firmou Contrato com a Agência Nacional de Transportes Terrestres, **DECLARO**, para fins de cumprimento de obrigações contratuais e sob pena das sanções administrativas, civis e penais, que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre os assuntos tratados, as atividades desenvolvidas e as ações realizadas no âmbito da

Agência Nacional de Transportes Terrestres, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

DECLARO, ainda, nos termos da Política de Segurança da Informação e Comunicações da Agência Nacional de Transportes Terrestres, Resolução nº 5.854, de 10 de setembro de 2019, ou outra que venha a substituí-la, estar ciente e **CONCORDO** com as condições abaixo especificadas, responsabilizando-me por:

I. tratar o(s) ativo(s) de informação como patrimônio da Agência Nacional de Transportes Terrestres;

II. utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Agência Nacional de Transportes Terrestres;

III. não utilizar ou divulgar em parte ou na totalidade, as informações de propriedade ou custodiadas, sob qualquer forma de armazenamento pela Agência Nacional de Transportes Terrestres, sem autorização prévia do gestor ou responsável pela informação;

IV. contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

V. utilizar credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Agência Nacional de Transportes Terrestres;

VI. responder, perante a Agência Nacional de Transportes Terrestres, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Cidade/UF, ____ de _____ de ____.

Nome do Funcionário

Cargo

CPF nº

Ciente:

Cidade-UF, ____ de _____ de ____.

Nome do Diretor ou representante legal da empresa
Cargo
CPF nº

-----FIM DO APÊNDICE "I"-----

APÊNDICE "J"**TERMO DE ENCERRAMENTO DO CONTRATO**

Processo Administrativo nº	Nº do Contrato	Data de Assinatura
Objeto		
Identificação da Empresa Contratada		
Nome da Empresa		
CNPJ	Inscrição Estadual	
Endereço		
Cidade	Estado	
CEP	Telefone	E-mail institucional

Por este instrumento, as partes abaixo identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O presente contrato está sendo encerrado por motivo de <motivo>.

As partes concedem-se mutuamente plena, geral, irrestrita e irrevogável quitação de todas as obrigações diretas e indiretas decorrentes do Contrato, não restando mais nada a reclamar de parte a parte, exceto as relacionadas no parágrafo a seguir.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização, mesmo após o encerramento do vínculo contratual:

- I. As obrigações relacionadas a processos iniciados de penalização contratual;

- II. As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais;
- III. A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados;
- IV. <inserir pendências, se houver>.

E assim, tendo lido e concordado com todos os seus termos, firmam as partes o presente instrumento, em duas vias iguais, para que surta seus efeitos jurídicos.

Cidade/UF, ____ de _____ de ____.

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

-----FIM DO APÊNDICE "J"-----