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
14/09/2022	1.0	Finalização da primeira versão do documento.	Equipe de planejamento da contratação
09/11/2022	2.0	Atualização do documento para inserir item de hardware	Equipe de planejamento da contratação
21/12/2022	3.0	Atendimento PARECER n. 00383/2022/PF-ANTT/PGF/AGU	Equipe de planejamento da contratação

SUMÁRIO

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de renovação de garantia e suporte da solução de inspeção de pacote de dados, para atender as necessidades da ANTT.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Lote	Item	Descrição	Unidade de Medida	Quantidade	CATSER	Valor Unitário (Máximo aceitável)	Valor Total (Máximo aceitável)
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2	27740	333.604,27	667.208,54
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2	27740	250.544,04	501.088,07
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1	27740	80.048,13	80.048,13
	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4	27502	145.708,98	582.835,91
	5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1	481647	620.456,41	620.456,41
	6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1	27740	370.628,10	370.628,10
VALOR TOTAL GLOBAL							**R$ 2.822.265,16**

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. A atualização e expansão da solução de inspeção de pacotes de dados é necessária pois tem como objetivo garantir a disponibilidade dos serviços de TI através da aquisição de solução de segurança para prevenir de ataques; evitar que usuários não autorizados acessem serviços ou

sistemas e controlar as ações realizadas na rede da ANTT; e prover linha de redundância para o enlace do Backbone principal.

3.1.2. Os equipamentos da solução de inspeção de pacotes de dados consistem em um dispositivo de rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software.

3.1.3. Esta solução controla todas as comunicações que passam de uma rede a outra e, em função do que sejam, permite ou denega seu passo. Para permitir ou denegar uma comunicação, a solução examina o tipo de serviço ao qual corresponde, que podem ser a sítios do tipo Portais (Terra, UOL, IG, por exemplo), correio eletrônico, dentre outros.

3.1.4. A solução de inspeção de pacotes de dados também é um grande aliado no combate a vírus e cavalos de Troia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados. Em redes corporativas, como a da ANTT, torna-se possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo rastrear e descobrir quais usuários as efetuaram.

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:

Planejamento Estratégico ANTT - 2020-2030			
ID	**Objetivo Estratégico**		
OPG4	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**
2.7	Solução de Inspeção de Pacotes de Dados, incluindo o fornecimento de equipamentos e softwares integrados em forma de *appliance* e/ou quando especificado; serviços de instalação e configuração, suporte técnico e garantia, serviços de operação assistida e demais serviços associados		Aprovado na Revisão do Planejamento Anual de Contratações - PAC 2022, nos termos da Deliberação nº 297/2022.

3.3. **Estimativa da demanda**

3.4. Para o correto dimensionamento da quantidade de bens e serviços a serem contratados, a equipe de planejamento da contratação considerou o quantitativo adquirido no Contrato nº 34/2017, bem como a necessidade de integração com a solução de microssegmentação da Cisco (ACI).

3.5. Assim sendo, a estimativa da demanda deverá observar os itens e quantitativos da tabela abaixo:

Item	**Descrição**	**Unidade de Medida**	**Quantidade**
1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2
2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2
3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1
4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4

5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1
6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1

3.6. **Parcelamento da Solução de TIC**

3.6.1. Os itens do objeto deverão ser licitados e adjudicados em lote, considerando a indivisibilidade dos mesmos, pois a soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

3.6.2. O agrupamento de itens irá garantir a qualidade técnica da solução não prejudicando a competividade do certame, já que há várias empresas no mercado de fornecimento da solução na forma agrupada.

3.7. **Resultados e Benefícios a Serem Alcançados**

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

a) Impedir o acesso não autorizado ao ambiente tecnológico da ANTT;

b) Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;

c) Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

d) Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet;

e) Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, dentre outros;

f) Criação de políticas de proteção da rede contra eventuais ataques de usuários mal-intencionados através do fechamento de portas não utilizadas, controlando a banda de internet a fim de evitar abusos em sua utilização.

4. **ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

4.1. **Requisitos de Negócio**

4.1.1. A presente contratação visa a manutenção e atualização da solução de inspeção de pacotes de dados do ambiente da ANTT, a fim de garantir a eficiência, continuidade e evolução da solução, compreendendo a realização de atividades de manutenção corretivas e preventivas que visem garantir o adequado funcionamento da ferramenta.

4.2. **Requisitos de Capacitação**

4.2.1. A solução já encontra-se implantada no ambiente tecnológico da ANTT. Dessa forma, não há necessidade de capacitação.

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. 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.

4.5. **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
Fornecimento das Licenças (Itens 1, 2 e 3)	Em até 15 (quinze) dias corridos a contar do recebimento da Ordem de Serviço (OS).
Serviços de Atualização e Suporte Técnico (Itens 1, 2, 3 e 4)	A partir do Termo de Recebimento Definitivo (TRD).
Fornecimento das Licenças (Item 4)	Em até 15 (quinze) dias corridos a contar do recebimento da Ordem de Serviço (OS).
Serviço de instalação e configuração (Item 4)	Em até 20 (vinte) dias corridos a contar do Termo de Recebimento Definitivo (TRD)
Fornecimento de equipamento (item 5), instalação e configuração (Itens 5 e 6)	Em até 60 (sessenta) dias corridos a contar do recebimento da Ordem de Fornecimento de Bens (OFB) e da Ordem de Serviço (OS).
Serviços de Atualização e Suporte Técnico (Item 6)	A partir do Termo de Recebimento Definitivo (TRD) do Item 5.

4.6. **Requisitos de Segurança e Privacidade**

4.6.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da ANTT.

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

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

4.7. **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:

a) baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;

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

c) maior eficiência na utilização de recursos naturais como água e energia;

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

e) maior vida útil e menor custo de manutenção de bens;

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

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

h) 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;

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

j) 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;

k) 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;

l) 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;

m) 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;

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

o) 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 CONTRATADA deverá prover a renovação da garantia técnica das licenças proprietárias e e fornecer a subscrição para o ambiente em nuvem, conforme tabela do subitem 2.1., desse TERMO DE REFERÊNCIA.

4.8.2. A renovação da garantia técnica dos produtos, referentes aos item 1 e 2, se dará pelo período de 12 (doze) meses, podendo ser prorrogada pelo mesmo período até o limite de 36 (trinta e seis) meses a critério da ANTT. A limitação da prorrogação desses itens está atrelada aos hardwares, que entrarão em end of support em 2025.

4.8.3. A renovação da garantia técnica dos produtos, referentes aos itens 3, 4 e 6, se dará pelo período de 12 (doze) meses, podendo ser prorrogada pelo mesmo período até o limite de 48 (quarenta e oito) meses a critério da ANTT.

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

4.9.1. A instalação dos itens 1, 2 e 3 terão um prazo máximo de até 15 (quinze) dias corridos, a partir do fornecimento dos itens; item 4 até 20 (vinte) dias corridos; itens 5 e 6 terão um prazo máximo de até 60 (sessenta) dias corridos.

4.9.2. A CONTRATADA procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos da ANTT, e, sendo posteriormente aferido e testado o seu perfeito funcionamento.

4.9.3. Compreende-se, nesta etapa, a instalação de hardware e softwares, módulos e aplicativos da solução fornecida pela CONTRATADA, bem como a atualização, renovação, ativação de licenças e funcionalidades previstas no objeto da contratação.

4.9.4. A CONTRATADA deve elaborar um documento de planejamento de instalação e implantação para aprovação da ANTT antes da execução da instalação.

4.9.5. A etapa de implantação deve acontecer de forma gradual e transparente, de acordo com a conveniência da ANTT.

4.9.6. Durante a implantação, a CONTRATADA deverá realizar, entre outras atividades:

a) Atualização inicial de software e/ou patches, caso necessário, para que a versão de instalação corresponda com a última versão válida disponibilizada pelo fabricante;

b) Configurações básicas;

c) Análise de performance;

d) Resolução de problemas.

4.9.7. Durante a etapa de implantação e migração, os PRODUTOS fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção.

4.9.8. Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de implantação e migração definidos pela ANTT.

4.9.9. Caberá à ANTT o acompanhamento implantação, fornecimento de informações sobre os equipamentos, sistemas e ferramentas existentes no ambiente, bem como a definição e concessão de janelas de intervenção.

4.9.10. As atividades de implantação deverão ser executadas em horário comercial.

4.9.11. A CONTRATADA deve garantir que a implantação não irá alterar as versões ou o funcionamento dos serviços instalados na unidade objeto da migração, sem a prévia autorização da ANTT.

4.9.12. A CONTRATADA deverá, com a supervisão da ANTT, planejar e realizar a instalação dos softwares e a configuração das funcionalidades com total interoperabilidade operacional com ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

4.9.13. Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como softwares, licenças e recursos humanos necessários à instalação e ativação das funcionalidades/licenças da solução.

4.9.14. A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação/migração e ao pleno funcionamento do ambiente de produção.

4.10. **Requisitos de Implantação**

4.10.1. Nos termos do subitem 4.5. que trata dos Requisitos Temporais.

4.11. **Requisitos de Garantia e Manutenção**

4.11.1. A CONTRATADA deverá prestar Serviço de Suporte Técnico remoto (on-line), no regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), contados da data de emissão do TERMO DE ACEITE DEFINITIVO, pelo período de 12 (doze) meses, observada a vigência contratual. Caso a CONTRATADA não consiga solucionar o problema de forma remota, deverá realizá-lo presencialmente (on-site), sem ônus adicionais para a ANTT.

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

4.11.2.1. Chamados ilimitados para o suporte on-line e on-site;

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

4.11.2.3. O suporte on-line (telefone e e-mail) deverá ser disponibilizado durante 24 (vinte e quatro) horas, 07 (sete) dias por semana e 365 (trezentos e sessenta dias) por ano;

4.11.2.4. O suporte on-line deverá disponibilizar ferramenta de acesso remoto e proporcionar o referido acesso quando solicitado, mediante autorização da ANTT.

4.11.3. Deverão ser cumpridos os prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadro abaixo:

Tabela de solução dos chamados			
Severidade	**Descrição**	**Tempo de 1° contato com cliente**	**Tempo de solução**
URGENTE	Serviço parado no ambiente de produção	30 Minutos	Em até 02 (duas) horas
MUITO IMPORTANTE	Erros ou problemas que impactam o ambiente de produção	60 Minutos	Em até 04 (quatro) horas
IMPORTANTE	Problemas contornáveis	90 Minutos	Em até 06 (seis) horas
RELEVANTE	Problemas com serviços não essenciais, que não impactam no negócio do cliente	120 minutos	Em até 08 (oito) horas
INFORMAÇÃO	Consulta técnica, dúvidas em geral, monitoramento.	150 Minutos	Em até 36 (trinta e seis) horas

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 do suporte técnico 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.

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. Controles apropriados devem ser realizados quando se enviar informações (logs/mensagens), isto é, devem ser verificadas as identidades de emissor e destinatário (sejam eles pessoas ou máquinas), assim como deve ser certificado se o conteúdo destas informações deve realmente ser compartilhado entre tais entes.

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

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

4.15.8. A solução deverá prever a geração de trilhas de auditoria para todas as operações de inclusão, exclusão, alteração de dados, desligamento do ambiente e alteração de configuração do sistema.

4.15.9. A CONTRATADA deverá realizar, quando solicitado e em conjunto com a ANTT, análise de impacto na privacidade dos dados pessoais relacionada ao objeto da contratação, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei 13.709/2018.

4.15.10. A CONTRATADA deverá realizar e apresentar à ANTT, quando solicitado, uma análise/avaliação de riscos dos recursos de processamento da informação, sistemas de segurança da informação e quaisquer outros ativos relacionados ao objeto do contrato, indicando o nível de risco ao qual o objeto do contrato e a ANTT está exposta, baseada em análise de vulnerabilidades, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela ANTT.

4.15.11. A CONTRATADA deverá utilizar recursos de segurança cibernética e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e, sempre que possível, em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a ANTT está exposta, considerando os critérios de aceitabilidade de riscos definidos pela ANTT.

4.15.12. A CONTRATADA deverá possuir e implementar processo de gestão de mudanças adequado para que mudanças na organização, nos processos de negócio e nos recursos de processamento da informação sejam controlados e não afetem a segurança cibernética, reduzindo o nível de risco ao qual o objeto do contrato e/ou a ANTT está exposta, considerando os critérios de aceitabilidade de riscos definidos pela ANTT.

4.15.13. A CONTRATADA deve possuir um processo de Gestão de Incidentes que registre os incidentes de segurança cibernética ocorridos e que guarde informações como: a descrição dos incidentes ou eventos, as informações e sistemas envolvidos, as medidas técnicas e de segurança utilizadas para a proteção das informações, os riscos relacionados ao incidente e as medidas tomadas para mitigá-los e evitar reincidências; além de implementar e manter controles e procedimentos específicos para detecção, tratamento e resposta a incidentes de segurança cibernética, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a ANTT está exposto, considerando os critérios de aceitabilidade de riscos definidos pela ANTT.

4.15.14. A CONTRATADA deve implementar os controles necessários para o registro de eventos e incidentes de segurança cibernética.

4.15.15. A CONTRATADA deve reportar de imediato à ANTT incidentes que envolvam vazamento de dados, fraude ou comprometimento da informação relacionados ao objeto do contrato.

4.15.16. A CONTRATADA deve implementar os controles necessários para coleta e preservação de evidências de incidentes de segurança.

4.15.17. A CONTRATADA deverá implementar controles de acesso baseado em uma política de controle de acesso para o objeto contratado, elaborada pela ANTT em conjunto com a CONTRATADA, tendo em vista o princípio do menor privilégio e a proteção adequada aos dados pessoais, de forma a reduzir o nível de risco ao qual o objeto e a ANTT estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela ANTT.

4.15.18. A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política. A política também deve definir situações e protocolos para acesso a informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos e que a ANTT julgar necessário.

4.15.19. A CONTRATADA deverá apresentar à ANTT, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança especificados, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

4.15.20. A CONTRATADA deverá disponibilizar todos os recursos necessários para que a CONTRATANTE, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança cibernética relacionadas ao objeto do contrato.

4.15.21. A CONTRATADA deve implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança cibernética, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à CONTRATANTE para fins de auditorias e inspeções.

4.15.22. A CONTRATADA deve implementar medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (logs) de suas próprias atividades.

4.15.23. A CONTRATADA deve implementar e manter controles e procedimentos específicos para assegurar o completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da CONTRATADA venham tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da solução objeto do contrato, cumprindo e fazendo cumprir o disposto nos acordos de confidencialidade firmados, partes integrantes deste documento.

4.15.24. A CONTRATADA deverá comunicar à ANTT, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

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 (OS) e da Ordem de Fornecimento de Bens (OFB)**

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

6.1.2.2. A OS/OFB 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/OFB 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/OFB.

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 papeis 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/Ordem de Fornecimento de Bens;

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

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.

7.3.7. O Gestor e/ou Fiscais do Contrato acompanharão a execução dos serviços prestados junto aos recursos disponibilizados pela CONTRATADA e emitirá Parecer Técnico com as atividades desenvolvidas.

IAE – INDICADOR DE ATRASO DE ENTREGA DE OS/OFB		
Tópico	**Descrição**	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Serviço/Ordem de Fornecimento de Bens.	
Meta a cumprir	**IAE < = 0**	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da Contratante e lista de Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS. Será subtraída a data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.	
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	**IAE = <u>TEX – TEST</u>** **TEST** Onde: **IAE** – Indicador de Atraso de Entrega da OS/OFB; **TEX** – Tempo de Execução – corresponde ao período de execução da OS/OFB, da sua data de início até a data de entrega dos produtos da OS/OFB. A data de início será aquela constante na OS/OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS/OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS/OFB continua a correr, findando-se apenas quanto a Contratada entrega os produtos da OS/OFB e haja aceitação por parte do fiscal técnico. **TEST** – Tempo Estimado para a execução da OS/OFB – constante na OS/OFB, conforme estipulado no Termo de Referência.	
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS/OFB de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.	
Início de Vigência	A partir da emissão da OS/OFB.	
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAE**: De 0 a 0,10 – Pagamento integral da OS/OFB; De 0,11 a 0,20 – Glosa de 0,5% sobre o valor da OS/OFB; De 0,21 a 0,30 – Glosa de 0,75% sobre o valor da OS/OFB; De 0,31 a 0,50 – Glosa de 1% sobre o valor da OS/OFB; De 0,51 a 1,00 – Glosa de 1,5% sobre o valor da OS/OFB;	

	Acima de 1 – Será aplicada Glosa de 3% sobre o valor da OS/OFB e multa de 10% sobre o valor do Contrato.

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:

a) falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas na contratação;

b) ensejar o retardamento da execução do objeto;

c) fraudar na execução do contrato;

d) comportar-se de modo inidôneo; ou

e) 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 8 horas 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. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.5.10. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.5.11. 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.

7.5.12. 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.

7.5.13. 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.

7.5.14. 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.

7.5.15. 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.

7.5.16. 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.

7.5.17. 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.

7.5.18. 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.

7.5.19. 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 x N x 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 =	$\frac{(6 / 100)}{365}$	I = 0,00016438 TX = Percentual da taxa anual = 6%

7.5.20. 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.

8. **ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO**

8.1. A contratação resta estimada em R$ 2.822.265,16 (dois milhões, oitocentos e vinte e dois mil duzentos e sessenta e cinco reais e dezesseis centavos), anual.

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
39250/393001	26.126.0032.218T.0001	44.90.52

9.2. Os pagamentos serão efetuados obedecendo aos seguintes critérios:

Descrição	Periodicidade	Condições de Pagamento
Licenciamento e Serviços de Renovação da Garantia Técnica	Parcela Única	Mediante a apresentação da Ordem de Serviço (OS) emitida, contendo o detalhamento do objeto, apresentação do Termo de Recebimento Definitivo e a apresentação da NF
Equipamento	Parcela Única	Mediante a apresentação da Ordem de Fornecimento de Bens (OFB) emitida, contendo o detalhamento do objeto, 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, limitado a 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, para os itens 3, 4 e 6.

10.2. Especificamente para os itens 1 e 2, o contrato vigorará por 12 (doze) meses, contados a partir da data da sua assinatura, podendo ser prorrogado por períodos iguais e sucessivos, limitado a 36 (trinta e seis) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Art. 57, da Lei nº 8.666, de 1993.

10.3. 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 irreajustáveis 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. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

11.6. 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.

11.7. 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.

11.8. 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 será de empreitada por preço global, 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. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades, previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

12.1.3. 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 por grupo.

12.1.4. 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.

12.1.5. 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 5° e 8° 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, em quantidades e características, no mínimo, 50% (cinquenta por cento), contendo as seguintes informações:

a) 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;

b) Indicação do CONTRATANTE de que foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);

c) Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação, considerando;

d) Data de emissão do atestado ou da certidão;

e) 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.

12.3.10. Para comprovação da experiência mínima de 12 (doze) meses será aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os 12 (doze) meses serem ininterruptos, conforme item 10.7.1 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

12.3.11. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MP n. 5/2017.

12.3.12. **Os critérios de aceitabilidade de preços serão:**

12.3.12.1. Valor Global: R$ 2.822.265,16 (dois milhões, oitocentos e vinte e dois mil duzentos e sessenta e cinco reais e dezesseis centavos), anual.

12.3.12.2. Valores unitários: conforme tabela do subitem 2.1. do Termo de Referência.

12.3.13. **O critério de julgamento da proposta é o menor preço global.**

12.3.14. **As regras de desempate entre propostas são as discriminadas no edital.**

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 prestadores dos serviços objeto desta contratação, que encontram-se aptas a atender as exigências de habilitação previstas neste TERMO DE REFERÊNCIA.

14. **ALTERAÇÃO SUBJETIVA**

14.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

15. **DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO**

15.1. A Equipe de Planejamento da Contratação foi instituída pelo Documento de Designação (SEI nº 12149406).

15.2. 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.

(Assinado eletronicamente) **JOÃO PROCÓPIO DO REGO NETO** Integrante Requisitante - Substituto	*(Assinado eletronicamente)* **VICTOR HUGO GOUVEIA DE LUCENA LIMA** Integrante Técnico	*(Assinado eletronicamente)* **THIAGO REIS VICTORINO** Integrante Administrativo

Aprovo, e declaro que está de acordo com a Instrução Normativa SGD/ME nº 1/2019, da Secretaria de Governo Digital do Ministério da Economia.

de

Autoridade Máxima da Área de TIC
(Assinado eletronicamente) **EUGENIO SOUTO PEREIRA** Superintendente de Tecnologia da Informação - Substituto

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 02/01/2023, às 18:28, 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 03/01/2023, às 12:12, 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 **EUGENIO SOUTO PEREIRA**, **Superintendente Substituto(a)**, em 16/01/2023, às 09:10, 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 **THIAGO REIS VICTORINO**, **Integrante Administrativo**, em 19/01/2023, às 16:35, 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 **14769323** e o código CRC **05EF0EEC**.

APÊNDICE "A"

REQUISITOS MÍNIMOS DA SOLUÇÃO

1. DESCRIÇÃO DOS REQUISITOS MÍNIMOS DA SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO

1.1. Contratação de expansão tecnológica para a solução de segurança de perímetro, abrangendo o fornecimento de equipamento, licenças e prestação de serviços de renovação de garantia e suporte técnico, para um período de 12 (doze) meses.

Lote	Item	Descrição	Unidade de Medida	Quantidade
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças para CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença para Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1
	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4

	5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1
	6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1

2. <u>ITENS 1, 2 e 3</u>

2.1. FUNCIONALIDADE DE FIREWALL

2.1.1. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

2.1.1.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames.

2.1.2. Realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

2.1.3. Deve suportar os seguintes tipos de NAT:

2.1.3.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente.

2.1.4. Enviar logs para sistemas de monitoração externos, simultaneamente;

2.1.5. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

2.1.6. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

2.1.7. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

2.1.8. Deve suportar NAT64.

2.1.9. Suportar OSPF graceful restart.

2.1.10. Deve permitir a segregação entre o plano de dados de gerenciamento do plano de dados de rede.

2.1.11. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, WEB, alterações de política e comunicação SNMP.

2.1.12. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, inclusive com a capacidade de aplicação de filtros personalizados. A ferramenta deve ter a opção de gravar o tráfego capturado em arquivos do tipo CAP, PCAP ou equivalente.

2.1.13. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3).

2.1.14. Deve possuir sistema de monitoramento em tempo real do hardware via interface gráfica, interface Web HTTPS e linha de comando CLI.

2.2. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

2.2.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.

2.2.2. Controle de políticas por usuários, grupos de usuários, IPs e redes.

2.2.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2.

2.2.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

2.2.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

2.2.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.

2.2.5.2. Reconhecer pelo menos 2.800 (Duas mil e oitocentos) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

2.2.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não.

2.2.7. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

2.2.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo.

2.2.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação.

2.2.10. Atualizar a base de assinaturas de aplicações automaticamente;

2.2.11. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD.

2.2.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários.

2.2.13. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística.

2.2.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

2.2.15. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

2.2.16. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

2.2.16.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.2.16.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes.

2.2.16.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local.

2.2.16.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

2.2.16.5. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário.

2.2.16.6. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs.

2.2.16.7. Suportar a criação de categorias de URLs customizadas.

2.2.16.8. Suportar a exclusão de URLs do bloqueio, por categoria.

2.2.16.9. Permitir a customização de página de bloqueio.

2.2.17. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede.

2.2.18. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou syslog, para a identificação de endereços IP e usuários.

2.2.19. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal).

2.3. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

2.3.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

2.3.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.

2.3.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo.

2.3.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

2.3.5. Detectar e bloquear a origem de portscans.

2.3.6. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações.

2.3.7. Possuir assinaturas para bloqueio de ataques de buffer overflow.

2.3.8. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, IMAP, SMB e FTP.

2.3.9. Suportar bloqueio de arquivos por tipo.

2.3.10. Identificar e bloquear comunicação com botnets.

2.3.11. Deve suportar referência cruzada com CVE.

2.3.12. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção.

2.3.13. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada.

2.3.14. Os eventos devem identificar o país de onde partiu a ameaça.

2.3.15. Suportar rastreamento de vírus em arquivos pdf.

2.3.16. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.).

2.3.17. Possuir a capacidade de prevenção de ameaças não conhecidas.

2.3.18. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado.

2.3.19. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

2.3.20. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT.

2.3.21. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

2.3.22. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado.

2.3.23. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL.

2.3.24. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas.

2.3.25. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2010, 2013 e 2016.

2.3.26. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente.

2.3.27. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização.

2.3.28. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada de forma independente das outras funcionalidades de segurança.

2.3.29. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

2.3.30. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP.

2.3.31. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm.

2.3.32. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo.

2.3.33. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração: 4.33.1. Número de arquivos emulados.

2.3.34. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

2.3.34.1. Arquivos scaneados;

2.3.34.2. Arquivos maliciosos.

2.4. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

2.4.1. Suportar a criação de políticas de QoS por:

2.4.1.1. Endereço de origem, endereço de destino e por porta;

2.4.2. O QoS deve possibilitar a definição de classes por:

2.4.2.1. Banda garantida, banda máxima e fila de prioridade;

2.4.2.2. Disponibilizar estatísticas RealTime para classes de QoS;

2.5. FUNCIONALIDADES DE VPN

2.5.1. Suportar VPN Site-to-Site e Cliente-To-Site.

2.5.2. Suportar IPSec VPN.

2.5.3. Suportar SSL VPN.

2.5.4. A VPN IPSEc deve suportar:

2.5.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES-XCBC, AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI.

2.5.5. A VPN SSL deve suportar:

2.5.5.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

2.5.5.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

2.5.5.3. Deve ser capaz de informar se a senha do usuário da VPN SSL autenticado via Microsoft Active Directory está próxima a expirar.

2.5.5.4. Atribuição de endereço IP nos clientes remotos de VPN.

2.5.5.5. Atribuição de DNS nos clientes remotos de VPN.

2.5.5.6. Suportar autenticação via AD/LDAP, certificado e base de usuários local.

2.5.5.7. Suportar leitura e verificação de CRL (certificate revocation list).

2.5.5.8. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Windows 7 e Windows 8.

3. <u>ITEM 4</u>

3.1. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA

3.1.1. A solução de segurança deve operar como um serviço vinculado à solução de microssegmentação da Cisco (ACI).

3.1.2. A solução deve realizar a inspeção do tráfego em camadas L4 a L7.

3.1.3. A solução deve contemplar funcionalidades de controle de acesso e segurança como funcionalidades de firewall, controle de aplicações e filtragem de URL's, prevenção de ameaças (IPS, Antivírus, Anti-bot, Antimalware), suporte para conexões VPN IPSec de forma integrada e simultânea, além de proteção à nível de sandboxing fornecendo proteção contra ataques de dia zero.

3.1.4. A solução deve realizar a inspeção do tráfego lateral (Leste e Oeste) direcionado ao serviço de microssegmentação do Cisco ACI.

3.1.5. A solução deve realizar a inspeção do tráfego Norte e Sul direcionado ao serviço.

3.1.6. A solução deve estar completamente licenciada para 4 leafs conectados ao APIC.

3.1.7. A solução deve ser capaz de importar objetos criados na solução do Cisco ACI para a console de gerenciamento de segurança.

3.1.8. A política de segurança deve refletir objetos, como EPG (End Point Groups) importados do Cisco ACI, de forma automática, e permitir com que eles possam ser utilizados dentro da política de controle de acesso.

3.1.9. A solução de gateway de segurança e gerência centralizada deverão permitir serem instaladas em máquinas virtuais.

3.1.10. No caso de solução via software, em caso de perda do ambiente, deverá ser possível que a própria CONTRATANTE consiga reestabelecer o firewall em outra máquina sem a necessidade de acionar a CONTRATADA, mesmo que necessário validação do licenciamento. Se a solução

ofertada for Appliance, deverá ser disponibilizada duas caixas com licença de High Availability (H.A), sendo aceito, no mínimo a solução Ativo x Passivo.

3.1.11. Em caso de solução software, deverá ser devidamente compatível e homologado, com Cisco ACI nas versões: 5.x, 4.x ,3.1(2*), 3.1(1*), 3.0(2*), 3.0(1*).

3.1.12. Em caso de licenciamento por software, todos os recursos hardware necessários para o pleno funcionamento da solução será provido pela CONTRATANTE, no caso de Appliance este deve ser fornecido pela CONTRATADA.

3.1.13. A solução deverá permitir expansão através de adição de novas licenças, de forma que suporte à criação de "pools" de gateways virtuais.

3.2. FUNCIONALIDADE DE FIREWALL

3.2.1. A solução deve consistir em funcionalidades de proteção de próxima geração.

3.2.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica.

3.2.3. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede.

3.2.4. Realizar upgrade via SCP, SFTP e https via interface WEB.

3.2.5. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

3.2.6. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames.

3.2.7. Deve suportar os seguintes tipos de NAT:

3.2.8. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente.

3.2.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

3.2.10. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.

3.2.11. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

3.2.12. Enviar logs para sistemas de monitoração externos, simultaneamente.

3.2.13. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção.

3.2.14. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

3.2.15. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.2.16. Autenticação integrada via Kerberos.

3.2.17. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP;

3.2.18. As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra.

3.2.19. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas.

3.2.20. A solução deve ter a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3).

3.2.21. Deverá suportar redundância e balanceamento de links, tendo capacidade mínima de 2 links de internet.

3.2.22. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

3.2.23. Deve permitir a configuração do tempo de checagem para cada um dos links.

3.3. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

3.3.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações.

3.3.2. Controle de políticas por usuários, grupos de usuários, IPs e redes.

3.3.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3.

3.3.4. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.3.4.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

3.3.4.2. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.3.4.3. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

3.3.4.4. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

3.3.4.5. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

3.3.5. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

3.3.6. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

3.3.7. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer);

3.3.8. Possuir mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador

da solução desejar bloquear apenas as subcategorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

3.3.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

3.3.10. Atualizar a base de assinaturas de aplicações automaticamente;

3.3.11. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

3.3.12. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

3.3.13. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

3.3.14. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

3.3.15. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.3.16. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

3.3.17. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

3.3.18. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.3.19. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

3.3.20. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

3.3.21. Suportar base ou cache de URLs local, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

3.3.22. Suportar a criação de categorias de URLs customizadas;

3.3.23. Suportar a exclusão de URLs do bloqueio, por categoria;

3.3.24. Permitir a customização de página de bloqueio;

3.3.25. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

3.3.26. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

3.3.27. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal).

3.4. FUNCIONALIDADE DE FILTRO DE DADOS

3.4.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

3.4.1.1. PCI - credit card numbers;

3.4.1.2. HIPAA - Medical Records Number – MRN;

3.4.1.3. International Bank Account Numbers – IBAN;

3.4.1.4. Source Code – JAVA;

3.4.1.5. U.S. Social Security Numbers - According to SSA;

3.4.1.6. Salary Survey Terms;

3.4.1.7. Viewer File – PDF;

3.4.1.8. Executable file;

3.4.1.9. Database file;

3.4.1.10. Document file;

3.4.1.11. Presentation file;

3.4.1.12. Spreadsheet file.

3.4.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

3.4.3. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

3.4.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

3.5. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

3.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall.

3.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos.

3.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo.

3.5.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

3.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo.

3.5.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

3.5.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP

Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.5.6.2. Detectar e bloquear a origem de portscans;

3.5.6.3. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

3.5.6.4. Possuir assinaturas para bloqueio de ataques de buffer overflow;

3.5.6.5. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

3.5.6.6. Suportar bloqueio de arquivos por tipo;

3.5.6.7. Identificar e bloquear comunicação com botnets;

3.5.6.8. Deve suportar referência cruzada com CVE;

3.5.7. Em cada proteção de segurança, deve estar incluso informações como:

3.5.7.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

3.5.7.2. Severidade;

3.5.7.3. Tipo de ação a ser executada.

3.5.8. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

3.5.9. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

3.5.10. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

3.5.11. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

3.5.12. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

3.5.13. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

3.5.14. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

3.5.15. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

3.5.16. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente;

3.5.17. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

3.5.18. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

3.5.19. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados;

3.5.20. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

3.5.21. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

3.5.22. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

3.5.23. A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

3.5.24. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

3.5.25. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

3.5.26. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

3.5.27. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

3.5.28. A solução deve permitir a criação de White Lists baseado no MD5 do arquivo;

3.5.29. Os eventos devem identificar o país de onde partiu a ameaça;

3.5.30. Suportar rastreamento de vírus em arquivos pdf;

3.5.31. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

3.5.32. Possuir a capacidade de prevenção de ameaças não conhecidas;

3.5.33. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada;

3.5.34. A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

3.5.35. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

3.5.36. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

3.5.37. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

3.5.38. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

3.5.39.

3.5.40. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede;

3.5.41. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

3.5.42. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

3.6. **FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO**

3.6.1. Suportar a criação de políticas de QoS por:

3.6.1.1. Endereço de origem, endereço de destino e por porta.

3.6.2. O QoS deve possibilitar a definição de classes por:

3.6.2.1. Banda garantida, banda máxima e fila de prioridade.

3.6.2.2. Disponibilizar estatísticas em tempo real para classes de QoS.

3.7. **FUNCIONALIDADES DE VPN**

3.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

3.7.2. Suportar IPSec VPN;

3.7.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

3.7.4. Suportar SSL VPN;

3.7.5. A solução de VPN Client-To-Site deve suportar e estar devidamente licenciada para 50 usuários simultâneos;

3.7.6. A VPN IPSEc deve suportar:

3.7.6.1. 3DES, Autenticação MD5, SHA-1 e SHA-2, Diffie-Hellman Group 1, Group 2, Group 5, Group 14 e Group 20, Algoritmo Internet Key Exchange (IKE) e IKE V2, AES 128 e 256 (Advanced Encryption Standard), SHA-256 e SHA-512 e Autenticação via certificado IKE PKI.

3.7.7. A VPN SSL deve suportar:

3.7.7.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

3.7.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

3.7.7.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

3.7.7.4. Atribuição de endereço IP nos clientes remotos de VPN;

3.7.7.5. Atribuição de DNS nos clientes remotos de VPN;

3.7.7.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

3.7.7.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

3.7.7.8. Suportar leitura e verificação de CRL (certificate revocation list);

3.7.7.9. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android.

3.7.8. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10, Windows 11 e MacOS X.

3.8. MÓDULO DE GERÊNCIA

3.8.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento.

3.8.2. A solução deverá ser gerenciada pelo mesmo sistema de gerenciamento das soluções de proteção de perímetro existente no órgão.

3.8.3. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, de, no mínimo 1 (um) mês.

3.8.4. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

3.8.5. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre.

3.8.6. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo.

3.8.7. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

3.8.8. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

3.8.9. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS).

3.8.10. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

3.8.11. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

3.8.12. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

3.8.13. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração.

3.8.14. Suportar backup das configurações e rollback de configuração para a última configuração salva.

3.8.15. Suportar validação de regras antes da aplicação.

3.8.16. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

3.8.17. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada.

3.8.18. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre.

3.8.19. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

3.8.20. Permitir a criação de certificados digitais para autenticação de usuários.

3.8.21. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).

3.8.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

3.8.23. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

3.8.24. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados.

3.8.25. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

3.8.26. Deve ser possível exportar os logs em CSV ou TXT.

3.8.27. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

3.8.28. Possibilitar rotação do log.

3.8.29. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

3.8.29.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego.

3.8.30. Deve permitir a criação de relatórios personalizados.

3.8.31. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5, 6 ou superior).

3.8.32. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI).

3.8.33. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações através de RestAPI.

3.8.34. Deve consolidar logs e relatórios de todos os dispositivos administrados.

3.8.35. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

3.8.36. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real.

3.8.37. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso.

3.8.38. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo:

3.8.38.1. ISO 27001 e ISO 27002;

3.8.38.2. PCI-DSS;

3.8.38.3. NIST 800-41;

3.8.38.4. GDPR (base da norma LGPD).

3.8.39. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição irá seguir. Não sendo permitido licenciamento mensal “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.

3.8.40. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.

3.8.41. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior.

3.8.42. Permitir a customização do padrão regulatório da própria instituição.

3.8.43. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança.

3.8.44. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados.

3.8.45. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual.

3.8.46. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança.

3.8.47. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação.

3.8.48. Possuir alertas de políticas e os potenciais violações de conformidade.

3.8.49. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança.

3.8.50. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real.

3.8.51. Permitir que os relatórios possam ser salvos, enviados e impressos.

3.8.52. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

3.8.53. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

3.8.54. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

3.8.55. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.8.56. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

3.8.57. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

3.8.58. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tantos gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

3.8.59. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

3.8.60. Criar certificados digitais para acesso dos usuários VPN;

3.8.61. Criar certificados digitais para VPNs Site-to-Site;

3.8.62. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

3.8.63. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

3.8.64. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição;

3.8.65. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma

única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

3.8.66. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

3.8.67. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes Pps e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

3.8.68. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

3.8.69. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

3.8.70. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

3.8.71. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

3.8.72. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

3.8.73. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

3.8.74. A solução deve ser capaz de personalizar e criar regras de correlação;

3.8.75. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

3.8.76. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

4. <u>ITENS 5 e 6</u>

4.1. REQUISITOS TÉCNICOS DA SOLUÇÃO DE PROTEÇÃO DE DDoS

4.1.1. REQUISITOS GERAIS

4.1.1.1. A solução DDoS deve ser um dispositivo dedicado e não uma função com licença em um Firewall, ou em um Balanceador.

4.1.1.2. Capacidade de mitigação: O sistema deve mitigar ataques DDoS ao menos a uma taxa mínima de 7.2 milhões de pacotes por segundo, sem bloquear ou afetar de maneira grave o tráfego legítimo. De igual forma, se exige uma capacidade mínima de mitigação em BW de 6Gbps e um desempenho de sessões concorrentes sob ataque ilimitado.

4.1.1.3. O sistema deve suportar mitigação de ataques SSL/TLS utilizando hardware dedicado, com Capacidade de tratar ao menos 20KCPS (RSA 2K).

4.1.1.4. O equipamento deve ter uma latência sob ataque menor ou igual a 60 microsegundos.

4.1.1.5. O sistema deve suportar mitigar ataques em IPv4 e IPv6.

4.1.1.6. O sistema, ao posicionar-se em linha, deverá ser completamente transparente, sem introduzir nenhuma alteração na rede. Adicionalmente, deve permitir habilitar “Interface grouping” ou “Interface tracking”, de tal forma que quando se desconecte uma porta, sua porta par também se desconecte, realizando assim a desconexão total do segmento que se está inspecionando de forma inline.

4.1.1.7. O sistema deve ter fontes redundantes e devem ser do tipo “hot-swap”.

4.1.2. CONECTIVIDADE E ÓTICAS

4.1.2.1. O equipamento deve contar com ao menos 2 portas com SFP+ para interconexão a 10Gbps futura.

4.1.2.2. O equipamento deve contar com proteção de ao menos 3 segmentos de cobre com bypass interno.

4.1.3. PROTEÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDO (DDOS)

4.1.3.1. O sistema deve proteger contra inundação de anomalias de pacotes. Ao menos:

a) Unrecognized L2 Format;
b) Incorrect IPv4 Checksum;
c) Invalid IPv4 Header or Total Length;
d) Invalid IP Header or Total Length;
e) Inconsistent IPv6 Headers;
f) Invalid L4 Header Length;
g) TTL Equal to 0;
h) IPv6 Hop Limit Reached;
i) Unsupported L4 Protocol;

j) Invalid TCP Flags;
k) Source or Dest. Address same as Local Host;
l) Source Address same as Dest Address (Land Attack).

4.1.3.2. Protecão contra ataques DDoS em camada de rede. Ao menos:

a) TCP-SYN floods;
b) TCP ACK + fim Flood;
c) TCP-SYN + ACK floods;
d) TCP-RESET floods;
e) TCP fragments flood;
f) UDP Floods;
g) UDP Fragmented Floods;
h) ICMP Floods;
i) IGMP Floods.

4.1.3.3. Proteção de ataques DDoS em camada de aplicação. Incluindo ao menos:

a) Todo tipo de ataques de tipo reflection, independente do protocolo camada 7 utilizado;
b) Todo tipo de ataques de tipo Amplification, independente do protocolo camada 7 utilizado;
c) DNS Floods;
d) HTTP Floods;
e) Low and SLow.

4.1.3.4. O sistema deve ter proteção DDoS originada de trás de CDN ou proxies.

4.1.3.5. O sistema deve ter mecanismos de proteção para ataques de tipo dia zero e ataques conhecidos.

4.1.3.6. O sistema deve ter mecanismo de prevenção de falsos positivos DDoS através de desafios e respostas. Como mínimo:

a) Desafios e respostas para TCP;
b) Desafios e resposta HTTP: 302 Redirect, Java Script;
c) Desafios e resposta em DNS.

4.1.3.7. O sistema deve ter protecão TCP Out-of–State Flood Attack

4.1.3.8. O sistema deve ter proteção granular para limitar por PPS e Kbps o tráfego enviado um destino com certos parâmetros definidos.

4.1.3.9. O sistema deve ter proteção contra ferramentas conhecidas de DoS.

4.1.4. ANÁLISE DE COMPORTAMENTO

4.1.4.1. O sistema deve proporcionar detecção de ataques DoS/DDoS em tempo real, baseado em Análise de Comportamento ou estatístico. Não se admitem soluções baseadas em limites estáticos de nenhum tipo já que se busca reduzir a quantidade de falsos positivos que possam existir na rede.

4.1.4.2. O sistema deve prevenir falsos positivos na detecção causados por flash crowds ou aumentos de tráfego súbito, através da correlação de parâmetros que variem com a taxa de tráfego com aqueles parâmetros que não variam com a taxa de tráfego.

4.1.4.3. Em fase de Proteção, O sistema deve atuar de forma automática, mitigando o ataque sem intervenção humana.

4.1.4.4. O sistema não deve realizar mitigação através de rate limits. A mitigação do ataque deve ser cirúrgica, unicamente bloqueando o tráfego que corresponda ao ataque e deixando passar o tráfego legítimo, ainda que o endereço IP de origem seja o mesmo do atacante.

4.1.4.5. O sistema deve suportar proteção comportamental ou estatística contra o mal uso da aplicação ou da red o contra ataques de DoS e DDoS. A proteção comportamental deve resultar na criação de uma contra-medida em tempo real para a mitigação dos ataques de forma imediata.

4.1.4.6. O sistema deve ter proteção contra vetores de ataques previamente desconhecidos

4.1.4.7. O sistema deve proteger contra ataques DDoS de tipo Burst utilizando Análise de Comportamento e mitigação cirúrgica automática, em tempo real.

4.1.4.8. O sistema deve basear sua decisão de bloqueio na informação de excesso de tráfego contida em Burst prévios e deve ser capaz de readaptar-se em caso de que o vetor de ataques DDoS no Burst varíe.

4.1.4.9. O sistema deve detectar e bloquear Comportamentos anômalos próprios de scans de IP e portas à rede, com o fim de prevenir a enumeração de recursos da entidade.

4.1.5. PROTEÇÃO DNS

4.1.5.1. O sistema deve suportar proteção DDoS DNS baseado em Análise de Comportamento de aplicação.

4.1.5.2. O sistema a nível de Análise de Comportamento ou estatístico DNS deve observar os seguintes parâmetros:

4.1.5.2.1. O sistema deve suportar um método de proteção de DNS mediante mecanismos de segurança positiva e negativa que permitam a proteção de ataques

4.1.5.2.2. O sistema deve suportar sistemas de proteção de DNS Challenge para limitar o tráfego malicioso mediante mecanismos de descarte de pacotes que reduzam os falsos positivos.

4.1.5.2.3. O sistema deve permitir crear listas brancas de subdomínios de forma manual ou automática.

4.1.5.3. A proteção de DNS deve ser completamente Stateless, Ingress-Only e não deve realizar contagens de NXDomains.

4.1.6. PROTEÇÃO SSL/TLS

4.1.6.1. A solução deve contar com hardware dedicado, o qual poderá ser interno ou externo, para o tratamento de tráfego SSL.

4.1.6.2. Proteção contra ataques DDoS Criptografados com SSL / TLS tanto na camada SSL como na camada HTTPS.

4.1.6.3. A solução deve poder autenticar sessões SSL com módulo de criptografia SSL para autenticar sessões legítimas e bloquear sessões de ataque criptografados por SSL.

4.1.6.4. A proteção SSL contra ataques de Negação de serviços, no deve cifrar/descifrar o tráfego quando não há ataque. A proteção só deve atuar em caso de ataque.

4.1.6.5. A proteção SSL deve funcionar em modo Ingress Only, sem necessidade de ver o tráfego que vem do servidor. Em outras palavras, a proteção deve ser Stateless.

4.1.6.6. O sistema deve habilitar flexibilidade com certificados wildcard de SSL, com o objeto de simplificar as operações e minimizar o número total de certificados administrados.

4.1.7. PERFIS DE GEOLOCALIZAÇÃO

4.1.7.1. A solução deve prover proteção de geolocalização que visualize os principais países atacantes de DDoS utilizando um mapa em tempo real.

4.1.7.2. A solução deve bloquear o tráfego de países específicos de imediato, com um clique de um botão na console de administração, utilizando um novo mapa de ataque dedicado, que apresente os principais países atacantes.

4.1.7.3. A solução de mitigação deve suportar dois modos de ativação de bloqueio: Sempre ativo e sob demanda.

4.1.7.4. A proteção deve admitir a configuração de listas de bloqueio/lista de permissões por objeto protegido, e que permita aos operadores da entidade a Capacidade de configurar rapidamente o bloqueio de país e as listas de permissões.

4.1.8. PROTEÇÃO CONTRA ATAQUES CONHECIDOS

4.1.8.1. A solução deve contar com um mecanismo de proteção de ataques DDoS lançados com ferramentas Conhecidas o que utilizem exploits conhecidos. Este mecanismo deve estar baseado em uma base de dados de assinaturas que contenha os parâmetros necessários para identificar estes ataques conhecidos.

4.1.8.2. As assinaturas devem ser atualizadas de forma automática através da internet durante a duração do suporte.

4.1.8.3. Ao ser a primeira linha de defesa, além de ataques DDoS Conhecidos deve proteger ao menos contra seguintes vulnerabilidades:

a) Web application vulnerabilities;
b) Mail server vulnerabilities;
c) FTP servers vulnerabilities;
d) DNS Vulnerabilities;
e) SQL Servers Vulnerabilities;
f) VoIP (SIP) vulnerabilities;
g) Buffer overflow.

4.1.9. REQUISITOS TÉCNICOS SISTEMA DE ADMINISTRAÇÃO CENTRALIZADA

4.1.9.1. O sistema deve suportar administração centralizada para toda A solução de DDoS.

4.1.9.2. O sistema deve ser tipo virtual appliance que permita instalar-se sobre Hyper-V ou VMware ESXi 5 ou superior na infraestrutura do cliente.

4.1.9.3. Deve-se incluir as licenças necessárias para poder ter Capacidade completa de realizar alterações e configurações da solução de mitigação de ataques.

4.1.9.4. O sistema deve suportar Web User interface para toda a configuração do dispositivo.

4.1.9.5. O sistema deve suportar um padrão industrial API para integração com aplicações personalizadas. A API deve ser oferecida sem custos.

4.1.9.6. A API deve estar completamente documentada.

4.1.9.7. A solução de administração deve prover a opção de personalizar "dashboards" por usuário, por política que mostrem informação em tempo real como: "top attacks view, traffic monitoring view, SLA reports (bandwidth consuming attack) view, etc".

4.1.9.8. O sistema deve suportar Acessos seguros HTTPS, SSH.

4.1.9.9. O sistema deve suportar o envio de eventos através de SYSLOG e SNMP.

4.1.9.10. O sistema deve suportar a configuração da solução através de scripts.

4.1.9.11. O sistema deve suportar RBAC para os administradores de múltiplos dispositivos.

4.1.9.12. O sistema deve suportar LDAP, RADIUS, TACACS e autenticação local.

4.1.9.13. O sistema deve suportar guardar toda a configuração em um servidor remoto.

4.1.9.14. O sistema deve suportar múltiplos administradores logados ao tempo na interface GUI.

4.1.9.15. O sistema deve suportar NTP.

4.1.9.16. O sistema deve gerar um alarme por cada alteração administrativa feita no dispositivo.

4.1.9.17. O sistema deve prover os MIBS completos.

4.1.9.18. O sistema deve suportar realização de backups por SCP, FTP, SFTP.

4.1.9.19. O sistema deve suportar ferramentas de diagnóstico como core dumps, arquivos de configuração, logs, etc.

4.1.9.20. O sistema deve suportar REST sobre HTTPS.

4.1.9.21. O sistema deve suportar a criação de scripts personalizados pela entidade que podem ser executados sobre múltiplos dispositivos ao mesmo tempo.

4.1.9.22. O sistema deve suportar relatórios históricos das soluções Anti DDoS.

4.1.9.23. Estes relatórios poderão ser programados e enviados de forma automática.

4.1.9.24. Deve contar com os seguintes protocolos para enviar os relatórios programados: via SFTP e SMTP.

4.1.9.25. Os seguintes são os formatos de relatórios que deve suportar o módulo de relatórios históricos: PDF, HTML, CSV, TEXT.

4.1.9.26. Deve contar com filtros granulares para personalizar o tipo e a informação nos relatórios.

4.1.9.27. Deve contar com relatórios out of the box, entre relatórios gerais de segurança e relatórios específicos da solução. Deve ter capacidade de gerar ao menos os seguintes relatórios:

a) Ataques por largura de banda;
b) Ataques por duração.
c) Ataques permitidos e negados;
d) Ataques críticos;
e) Relatórios de tipo TOP:
    a. Destinos;
    b. Origem;
    c. Aplicação.

---------- FIM DO APÊNDICE “A” ----------

SUTEC SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ANTT AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

APÊNDICE "B"

MODELO

PROPOSTA DE PREÇOS

(em papel timbrado da empresa)

À
AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES
Superintendência de Gestão Administrativa – 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 aquisição (ou contratação) xxxxxxxx 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

Lote	Item	Descrição	Unidade de Medida	Quantidade	Valor Unitário	Valor Total
1	1	Contratação de serviço de renovação de suporte técnico e garantia das licenças de CheckPoint 15400 NGTX Appliance da ANTT, pelo período de 12 (doze) meses.	Serviço	2		
	2	Contratação de serviço de renovação de suporte técnico e garantia das licenças de CheckPoint 5800 NGTX Appliance da ANTT pelo período de 12 (doze) meses.	Serviço	2		
	3	Contratação de serviço de renovação de suporte técnico e garantia da licença de Security Management Software da ANTT, pelo período de 12 (doze) meses.	Serviço	1		

	4	Fornecimento de licenças para solução de segurança integrada à solução de rede definida por software (SDN) Cisco ACI, com serviço de suporte técnico e atualização pelo período de 12 (doze) meses.	Serviço	4		
	5	Fornecimento e instalação de solução de proteção contra ataques de serviços DDoS	Unidade	1		
	6	Suporte técnico e garantia pelo período de 12 (doze) meses, para solução de proteção contra ataques de serviços DDoS.	Serviço	1		
VALOR TOTAL GLOBAL						**R$ -**

1) Dados da Proposta:

Valor Total: R$ _____ (**VALOR POR EXTENSO**).

SOFTWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos softwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Software: _____ Versão: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [ ] 2. Importado: [ ]

Sítio na WEB do Fabricante: _____

Responsável: _____Telefone Contato: _____

HARDWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos hardwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Hardware: _____ Marca: _____ Modelo: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [ ] 2. Importado: [ ]

Sítio na WEB do Fabricante: _____

Responsável: _____Telefone Contato: _____

2) Validade da Proposta: 90 (noventa) 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, ainda, que inexiste 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” ----------

SUTEC SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ANTT AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

APÊNDICE "C"

MODELO

ORDEM DE SERVIÇO (OS) /ORDEM DE FORNECIMENTO DE BENS (OFB)

N° da Ordem de Serviço	Data de Emissão da OS	N° do Contrato	Data de Assinatura do Contrato

Área Requisitante	Requisitante Responsável

1. IDENTIFICAÇÃO DA EMPRESA CONTRATADA

Nome da Empresa		
CNPJ		**Inscrição Estadual**
Endereço		
Cidade		**Estado**
CEP	**Telefone**	**E-mail institucional**
Preposto		

2. OBJETO DO CONTRATO

XXXXXXXXXXXXX

2.1. ESPECIFICAÇÃO DOS SERVIÇOS A SEREM EXECUTADOS E CUSTOS ESTIMADOS

Item	Descrição	Unidade	Quantidade	Valor Unitário R$	Valor Total R$
1					
2					
3					
4					
				VALOR TOTAL DA OS R$	

2.2. DETALHAMENTO DOS SERVIÇOS A SEREM EXECUTADOS E DAS ENTREGAS

2.3. PERÍODO DE EXECUÇÃO DOS SERVIÇOS

Data de Início da Execução	____/____/_____	Data de Término da Execução	____/____/_____

3. LOCAL DE EXECUÇÃO DOS SERVIÇOS

Os serviços deverão ser executados, conforme definido no Termo de Referência.

4. APROVAÇÃO DO GESTOR DO CONTRATO

Solicitação

Solicitamos a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

(assinado eletronicamente)
<Nome do Fiscal Requisitante>
Matrícula SIAPE <Nº da matrícula>
Fiscal Requisitante

Autorização
Autorizo a realização do serviço acima caracterizado, nos termos constantes desta Ordem de Serviços, que tem por base as obrigações e responsabilidades da contratada constantes do contrato firmado, supra indicado.

(assinado eletronicamente)
<Nome do Gestor do Contrato >
Matrícula SIAPE <Nº da matrícula>
Gestor do Contrato

5. CIENTE DA CONTRATADA

Declaramos nossa ciência e concordância com as condições registradas nesta Ordem de Serviços para execução dos serviços solicitados.

(assinado eletronicamente)
<Nome do Representante Legal da Contratada>
CPF:
Preposto da Contratada

---------- FIM DO APÊNDICE "C" ----------

SUTEC SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ANTT AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

APÊNDICE "D"

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 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	N° 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"** ----------

SUTEC SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ANTT AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

APÊNDICE "F"

MODELO

TERMO DE RECEBIMENTO PROVISÓRIO

IDENTIFICAÇÃO

N° do Contrato	Número da O.S.	Data de Emissão
Contratante		
Contratada		
Processo Administrativo nº	**Processo Licitatório**	
Objeto		

ESPECIFICAÇÃO DOS SERVIÇOS E VOLUME DE EXECUÇÃO

Lote	Item	Descrição dos Serviços	Unidade	Quantidade	Valor Unit. (R$)	Valor Total (R$)
1	1					
	2					
	3					
	4					
	...					
					VALOR TOTAL (R$)	

RECEBIMENTO

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso II, alínea "a", da Instrução Normativa SGD/ME nº 1/2019, de 4 de abril de 2019, alterada pela IN SGD/ME nº 31/2021, emitida pela Secretaria de Governo Digital do Ministério da Economia, que os serviços, integrantes da O.S. acima identificada e/ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos provisoriamente nesta data e serão objetos 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 após a verificação dos requisitos e demais condições contratuais, no prazo de até 15 (quinze) dias, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**.

PELA CONTRATANTE:

(assinado eletronicamente)
<Nome do Fiscal Técnico>
Matrícula SIAPE <Nº da matrícula>
Fiscal Técnico

PELA CONTRATADA:

(assinado eletronicamente)
<Nome do Representante Legal da Contratada>
CPF:
Preposto da Contratada

---------- FIM DO APÊNDICE "F" ----------

SUTEC SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ANTT AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES

APÊNDICE "G"

MODELO

TERMO DE RECEBIMENTO DEFINITIVO

IDENTIFICAÇÃO

N° do Contrato	Número da O.S.	Data de Emissão

Contratante
Contratada

Processo Administrativo nº	Processo Licitatório

Objeto

ESPECIFICAÇÃO DOS SERVIÇOS E VOLUME DE EXECUÇÃO

Lote	Item	Descrição dos Serviços	Unidade	Quantidade	Valor Unit. (R$)	Valor Total (R$)
1	1					
	2					
	3					
	4					
	...					
					VALOR TOTAL (R$)	

ATESTE DE RECEBIMENTO

Por este instrumento, atestamos para fins de cumprimento do disposto na alínea "f", inciso II, e alínea "d", inciso III, do art. 33, da Instrução Normativa SGD/ME nº 1/2019, de 4 de abril de 2019, alterada pela IN SGD/ME nº 31/2021, emitida pela Secretaria de Governo Digital do Ministério da Economia, que os serviços integrantes da O.S. acima identificada e/ou conforme definido no Modelo de Execução do contrato supracitado, atendem às exigências especificadas no Termo de Referência e do Contrato, com base no Relatório Circunstanciado elaborado pela fiscalização técnica e documentação apresentada.

DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <O.S.> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº _____ ou Nota Técnica nº _____>.

PELA CONTRATANTE:

(assinado eletronicamente)
<Nome do Fiscal Requisitante>
Matrícula SIAPE <Nº da matrícula>
Fiscal Requisitante

(assinado eletronicamente)
<Nome do Fiscal Técnico>
Matrícula SIAPE <Nº da matrícula>
Fiscal Técnico

PELA CONTRATADA:

(assinado eletronicamente)
<Nome do Representante Legal da Contratada>
CPF:
Preposto da Contratada

---------- FIM DO APÊNDICE "G" ----------

APÊNDICE "H"

MODELO

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 Contratação de Serviços de Outsourcing de Impressão, 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>>

TESTEMUNHAS

_____ _____

<Nome>
<Qualificação>
<CPF>

<Nome>
<Qualificação>
<CPF>

<Local>, <dia> de <mês> de <ano>.

---------- FIM DO APÊNDICE "H" ----------

APÊNDICE "I"

MODELO

TERMO DE CIÊNCIA

Processo Administrativo nº	N° 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 substitui-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"

MODELO

TERMO DE ENCERRAMENTO DO CONTRATO

IDENTIFICAÇÃO

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

LISTA DE VERIFICAÇÃO

Item	ATENDIDO	NÃO ATENDIDO	NÃO APLICÁVEL
Os recursos humanos e materiais foram preparados para a continuidade do negócio por parte da Administração?			
A contratada entregou as versões finais dos produtos e a documentação?			
Houve a transferência final de conhecimentos sobre a execução e manutenção da solução?			
A contratada devolveu os recursos que foram oferecidos para operacionalizar o contrato?			
Foram revogados os perfis de acesso dos funcionários da contratada?			
Foram eliminadas as caixas postais que foram oferecidas à contratada?			
<outras que se apliquem ao objeto da contratação>			
...			

DO ENCERRAMENTO

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 _____.

PELA CONTRATANTE:

(assinado eletronicamente)
<Autoridade Competente da Área Administrativa>
Matrícula SIAPE <Nº da matrícula>

PELA CONTRATADA:

(assinado eletronicamente)
<Nome do Representante Legal da Contratada>
CPF:
Preposto da Contratada

---------- **FIM DO APÊNDICE "J"**----------