PREGÃO ELETRÔNICO

90006/2025

CONTRATANTE (UASG)

Agência Nacional da Aviação Civil (113214)

OBJETO

Serviços técnicos especializados de Segurança da Informação para a implantação de um Security Operation Center - SOC, envolvendo serviços de gerenciamento, monitoramento, detecção e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de ativos e configuração segura, de gestão de conta, controle de acesso e auditoria, de apoio à gestão de segurança, serviços de inteligência de ameaças cibernéticas e de testes de invasão, pelo período de 24 (vinte e quatro) meses, na forma de serviços continuados, executados sem dedicação exclusiva de mão de obra.

VALOR TOTAL DA CONTRATAÇÃO

R$ 9.184.874,58 (nove milhões, cento e oitenta e quatro mil oitocentos e setenta e quatro reais e cinquenta e oito centavos)

DATA DA SESSÃO PÚBLICA

Dia 15/05/2025 às 10hs (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

menor preço por grupo

MODO DE DISPUTA:

aberto e fechado

Baixe o APP Compras.gov.br
e apresente sua proposta!

ÍNDICE

ANAC
SCS, Quadra 09, Lote C, Torre A - 3º Andar, Edifício Parque Cidade Corporate - Bairro Setor Comercial Sul, Brasília/DF, CEP 70308-200 - www.anac.gov.br

PREGÃO ELETRÔNICO

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

PREGÃO ELETRÔNICO Nº 90006/2025

Processo nº 00058.007264/2023-23

Torna-se público que a AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL, por meio da Gerência Técnica de Licitações e Contratos, sediada no Setor Comercial Sul, Quadra 09, Lote C, Ed. Parque Cidade Corporate, Torre A, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de solução de tecnologia da informação e comunicação para prestação de serviços técnicos especializados de Segurança da Informação para a implantação de um *Security Operation Center* - SOC, envolvendo serviços de gerenciamento, monitoramento, detecção e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de ativos e configuração segura, de gestão de conta, controle de acesso e auditoria, de apoio à gestão de segurança, serviços de inteligência de ameaças cibernéticas e de testes de invasão, pelo período de 24 (vinte e quatro) meses, na forma de serviços continuados, executados sem dedicação exclusiva de mão de obra, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em um grupo, formado por dez itens, além de dois itens avulsos - item 11 e item 12, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação no grupo e/ou nos itens avulsos conforme seu interesse, devendo oferecer proposta para todos os itens que compõem o grupo em caso de participação neste. Destaca-se, ainda, a necessidade de contratar fornecedores distintos para o Grupo 1 e o item 12, dada a necessidade de autonomia entre os serviços, conforme especifica o item 8.4.9. do Termo de Referência.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou

entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de

agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.13.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor unitário e total do item;

4.1.2. Quantidade cotada.

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.2.1. O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos

previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.8.1. O prazo de validade da proposta não será inferior a **60 (sessenta)** dias**,** a contar da data de sua apresentação.

4.8.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.8.3. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos.

4.9. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá

ser de R$ 10,00 (dez reais).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa adotado.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

5.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

5.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.12.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.12.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “fechado e aberto”, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

5.13.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

5.13.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de

dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.13.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

5.14. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.15. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.16. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.17. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.18. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.20.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.20.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.20.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.20.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.21. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

5.21.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

5.21.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

5.21.1.2. bens e serviços com tecnologia desenvolvida no País; e

5.21.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

5.21.2. Os licitantes classificados que estejam enquadrados no item 5.21.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

5.21.3. Caso a preferência não seja exercida na forma do item 5.21.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 5.21.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.21.1.3 caso esse direito não seja exercido.

5.21.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

5.22. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.22.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.22.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.22.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.22.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.22.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.22.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.22.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.22.2.2. empresas brasileiras;

5.22.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.22.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.23.1. Tratando-se de licitação em grupo, a contratação posterior de item específico do grupo exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade e serão observados os preços unitários máximos informados no Termo de Referência como critério de aceitabilidade.

5.23.2. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

5.23.3. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela

Administração.

5.23.4. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.23.5. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.23.6. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.23.7. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 3.6 deste edital.

6.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.6. Será desclassificada a proposta vencedora que:

6.6.1. contiver vícios insanáveis;

6.6.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.7.1. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do pregoeiro, que comprove:

6.7.2. que o custo do licitante ultrapassa o valor da proposta; e

6.7.3. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.9. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

7.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o Termo de Referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

7.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

7.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.9. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.10. Considerando que na presente contratação a avaliação prévia do local de execução é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, o licitante deve atestar, sob pena de inabilitação, que conhece o local e as condições de realização do serviço, assegurado a ele o direito de realização de vistoria prévia.

7.10.1. O licitante que optar por realizar vistoria prévia terá disponibilizado pela Administração data e horário exclusivos, a ser agendado através do telefone (61) 3314-4213 ou pelo e-mail std@anac.gov.br, cujo campo “Assunto” da mensagem deverá conter o texto “Vistoria – Edital 90006/2025” com no mínimo 48 horas úteis de antecedência, de modo que seu agendamento não coincida com o agendamento de outros licitantes.

7.10.2. Caso o licitante opte por não realizar vistoria, deverá apresentar a Declaração de responsabilidade de não vistoriar, conforme o ANEXO - DECLARAÇÃO DE RESPONSABILIDADE DE NÃO VISTORIA do Termo de Referência, juntamente com os documentos de habilitação.

7.11. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.11.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.12. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.12.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.13. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.13.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.14. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.14.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.14.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

7.15. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.15.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.15.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.16. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.17. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.13.1.

7.18. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.19. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.20. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.3.3. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.gov.br/anac/pt-br/sistemas/protocolo-eletronico-sei/pesquisa-publica-de-processos-e-documentos.

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo e-mail **licitacao@anac.gov.br.**

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico Licitações e Contratos — Agência Nacional de Aviação Civil (Anac)

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência;

11.11.1.1. Anexo ao Termo de Referência - Especificações Técnicas

11.11.1.2. Anexo ao Termo de Referência - Ambiente Tecnológico

11.11.1.3. Anexo ao Termo de Referência - Catálogo de Serviços

11.11.1.4. Anexo ao Termo de Referência - Termo de Compromisso de Manutenção de

Sigilo

11.11.1.5. Anexo ao Termo de Referência - Termo de Ciência

11.11.1.6. Anexo ao Termo de Referência - Ordem de Serviço

11.11.1.7. Anexo ao Termo de Referência - Termo de Recebimento Provisório de Serviços

11.11.1.8. Anexo ao Termo de Referência - Termo de Recebimento Definitivo

11.11.1.9. Anexo ao Termo de Referência - Modelo de Proposta Comercial

11.11.1.10. Anexo ao Termo de Referência - Declaração de Responsabilidade

11.11.2. ANEXO II - Minuta de Contrato.

Brasília, 28 de abril de 2025

Bruno Silva Fiorillo

Pregoeiro

Documento assinado eletronicamente por **Bruno Silva Fiorillo**, **Pregoeiro(a)**, em 28/04/2025, às 14:44, conforme horário oficial de Brasília, com fundamento no art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.anac.gov.br/sei/autenticidade, informando o código verificador **11467929** e o código CRC **CAAEF31C**.

Referência: Processo nº 00058.007264/2023-23 SEI nº 11467929

Termo de Referência 9/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
9/2024	113214-AGENCIA NACIONAL DE AVIACAO CIVIL - ANAC	REGINALDO LIRA DE ARAUJO	15/04/2025 09:36 (v 3.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC	90044/2023	00058.007264/2023-23

1. Definição do objeto

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de serviços técnicos especializados de Segurança da Informação para a implantação de um Security Operation Center - SOC, envolvendo a prestação de serviços de gerenciamento, monitoramento, detecção e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de ativos e configuração segura, de gestão de conta, controle de acesso e auditoria, de apoio à gestão de segurança, serviços de inteligência de ameaças cibernéticas e de testes de invasão , pelo período de 24 (vinte e quatro) meses, na forma de serviços continuados, executados sem dedicação exclusiva de mão de obra, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Tabela 1.1

Grupo	Item	Especificação	CATSER	Unidade de Medida	Quantidade	Valor Unitário R$	Valor Total R$
1	1	Apoio à Gestão de Segurança	27014	Mensal	24 meses	40.529,86	972.716,64
	2	Gestão de Ativos e Configuração Segura	27014	Mensal	24 meses	19.554,94	469.318,56
	3	Gestão de Conta, Controle de Acesso e Auditoria	27014	Mensal	24 meses	19.554,94	469.318,56
	4	Gestão de incidentes de segurança da informação (Blue Team)	27014	Mensal	24 meses	46.529,04	1.116.697,06
	5	Monitoramento e correlação de eventos de segurança da informação	27014	Mensal	24 meses	47.158,19	1.131.796,56
	6	Serviço de contratação de pacotes adicionais de 500 EPS da ferramenta SIEM por 12 meses	27014	Sob demanda	10	8.000,00	80.000,00
	7	Gestão de vulnerabilidades	27014	Mensal	24 meses	27.488,50	659.724,00

	8	Solução de gerenciamento de vulnerabilidades de segurança	27014	Mensal	24 meses	6.000,00	144.000,00
	9	Segurança de Redes	27014	Mensal	24 meses	27.488,50	659.724,00
	10	Segurança de Aplicação	27014	Mensal	24 meses	27.488,50	659.724,00
2	**11**	Inteligência de Ameaças Cibernéticas	27014	Mensal	24 meses	32.000,00	768.000,00
3	**12**	Testes de Invasão	27014	Sob demanda	240	8.557,73	2.053.855,20

1.2. Os serviços objeto desta contratação são caracterizados como comuns, uma vez podem ser definidos no edital por meio de especificações objetivas e que são adequadas a estabelecer o padrão de qualidade desejado, de acordo com características usuais no mercado. Assim, tendo em vista tais características usuais, os serviços podem ser ofertados por diversos fornecedores que podem atender às referidas especificações objetivas.

1.3. O prazo de vigência da contratação é de 24 (vinte e quatro) meses, contados da data de assinatura pelo CONTRATANTE e prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.4 No tocante aos itens relativos aos serviços técnicos especializados de Segurança da Informação, o serviço é enquadrado como continuado, tendo em vista que sua interrupção pode comprometer a continuidade e segurança dos serviços prestados pela Agência. Nesse sentido, é necessária uma estrutura organizacional que possa se responsabilizar por ameaças à segurança e criar processos eficientes para monitorar, detectar, analisar, responder e restaurar atividades eventualmente comprometidas por ataques cibernéticos.

1.5 Dessa forma, considera-se vantajoso para a administração pública que a vigência contratual seja de 24 (vinte e quatro) meses. A prorrogação do contrato, nos termos e prazos da Lei nº 14.133/2021, dependerá da verificação da manutenção da necessidade, economicidade e oportunidade da contratação, acompanhada da realização de pesquisa de mercado que demonstrará a vantajosidade dos preços contratados para a Administração.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.7 O objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 94/2022.

1.8 A contratação está em consonância com os documentos estratégicos elencados no art. 6º da IN SGD/ME nº 94/2022.

2. Fundamentação da contratação

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está aprovado no Planejamento e Gerenciamento das Contratações - PGC e publicado no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

I) ID PCA no PNCP: **07947821000189-0-000001/2025**

II) Data de publicação no PNCP: **05/03/2025**

III) Id do item no PCA: 62

IV) Classe/Grupo: **165 - SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃOE COMUNICAÇÃO (TIC), NAO CLASSIFICADOS EM OUTROS TÓPICOS**

V) Identificador da Futura Contratação: **113214-57/2025**

3. Descrição da solução

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.
3.2. A solução de TIC consiste em serviços gerenciados de segurança da informação, divididos em três Grupos.

3.3. **Grupo 01, Segurança Defensiva**, composto pelos seguintes itens:
3.3.1. Apoio a Gestão de Segurança: tem por objetivo oferecer um conjunto abrangente de soluções, avaliações e revisões relacionados à segurança da informação, tendo por fundamento os normativos e frameworks de segurança, em especial o CIS Controls. Esse serviço fornece uma visão detalhada da postura de segurança da organização, identificando lacunas e vulnerabilidades, oferecendo orientações estratégicas para fortalecer as defesas e responder de forma eficiente a incidentes cibernéticos, garantindo assim a proteção contínua dos ativos e dados críticos da empresa, além de contribuir para identificar e mitigar as ameaças cibernéticas mais pertinentes ao ambiente da CONTRATANTE. Contempla, entre outros, a elaboração e revisão de políticas, diretrizes e cartilhas de segurança da informação, o acompanhamento das ações demandadas pelos normativos e pelas orientações elaborados pelo Gabinete de Segurança Institucional - GSI e pela Secretaria de Governança Digital - SGD, assim como das ações relacionadas ao Programa de Privacidade e Segurança da Informação- PPSI/SGD.
3.3.2. Gestão de Ativos e Configuração Segura: tem por objetivo oferecer um conjunto abrangente de soluções e assessment, tendo por base os respectivos normativos e controles do PPSI, para fornecer um conjunto de medidas prioritárias e acionáveis que a CONTRATANTE pode implementar para melhorar sua postura de segurança cibernética. Esses serviços fornecem uma visão detalhada da postura de segurança da organização, trazendo maturidade aos usuários da CONTRATANTE com conscientização, controle de acesso e aspectos essenciais da segurança da informação com orientações estratégicas.
3.3.3. Gestão de Conta, Controle de Acesso e Auditoria: tem por objetivo oferecer uma solução integral para gerenciar de forma segura as credenciais de acesso e as permissões de usuários com privilégios elevados dentro do ambiente da CONTRATANTE, utilizando como referências os respectivos controles do PPSI e normativos correlatos.
3.3.4. Monitoramento e Gestão de Incidentes de Segurança: os serviços mantidos por esta categoria se darão de forma proativa e contínua, baseando-se no resultado do monitoramento dos logs mantidos pela ferramenta SIEM (Security Information Event Management), mas não limitantes a ela. Os serviços não se limitarão apenas na observância dos logs gerados, mas também na evolução constante das capacidades de observação da ferramenta de monitoramento. Para o atendimento desse serviço, a CONTRATADA deverá disponibilizar ferramenta de SIEM , a ser precificada junto aos itens 9 e 10 do Grupo 1, com os requisitos descritos no Anexo I - Especificações Técnicas dos Serviços.
3.3.5. Gestão de Vulnerabilidade: tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do CONTRATANTE, a fim de evitar que ataques cibernéticos direcionados ao CONTRATANTE obtenham sucesso, explorando tais vulnerabilidades já conhecidas. O serviço também contempla a gestão de vulnerabilidade. Para o atendimento desse serviço, a CONTRATADA deverá disponibilizar solução de Gerenciamento de Vulnerabilidades, a ser precificada junto ao item 8 do Grupo 1, com os requisitos descritos no Anexo I - Especificações Técnicas dos Serviços.
3.3.6. Segurança de Redes e Segurança da Aplicação: têm por objetivo oferecer uma vigilância proativa sobre a infraestrutura de segurança da informação da CONTRATANTE, garantindo a o funcionamento das tecnologias do ambiente. Com uma equipe especializada, os analistas de segurança monitorarão constantemente as ferramentas listadas no ANEXO II – Ambiente Tecnológico, garantindo a operação e sustentação destes sistemas e tecnologias, assim como o atendimento de requisições realizadas via portal de serviços.

3.4. **Grupo 2, Inteligência de Ameaças**: esse serviço consiste em verificar fontes disponíveis na Internet - tanto as acessadas abertamente quanto as chamadas deep e dark web - em busca de potenciais ameaças cibernéticas à instituição CONTRATANTE.

3.5. **Grupo 3, Testes de Invasão:** este serviço tem por objetivo atuar de forma proativa e continua para identificar, mapear, documentar as vulnerabilidades nos sistemas, aplicações, containers, máquinas virtuais, processos e ativos de segurança tecnológica através da realização de “PENTEST” (Teste de penetração na infraestrutura e aplicações Web) abrangendo todos os ativos de infraestrutura de tecnologia da ANAC.

3.6. **Parcelamento da Solução de TIC**

A pretensa contratação não se trata de uma única solução de TIC. Para isso, os serviços foram segmentados em três lotes – Segurança Defensiva, Inteligência de Ameaças e Testes de Invasão – considerando as especificidades de cada um, incluindo métricas, especialização das equipes e formas de mensuração das atividades. Essa segmentação amplia a participação de empresas especializadas no processo de licitação.

Os Testes de Invasão simulam ataques ao ambiente da ANAC e, por sua natureza, devem ser conduzidos por uma empresa distinta daquela responsável pela Segurança Defensiva. Isso garante imparcialidade e eficácia nas avaliações. Além disso, a utilização de diferentes metodologias e abordagens de ataque permite a identificação mais abrangente de vulnerabilidades, possibilitando a adoção de medidas corretivas eficazes.

Já os serviços de Inteligência de Ameaças Cibernéticas têm como objetivo fornecer informações detalhadas para prevenção e combate a ameaças. Para garantir imparcialidade e aumentar a confiabilidade das informações geradas, é recomendável que esses serviços sejam realizados por uma empresa independente. Essa abordagem permite a obtenção de insights mais objetivos e não tendenciosos, aprimorando as estratégias de defesa da ANAC.

A decisão de agrupar os 10 itens dentro do Lote 1 (Segurança Defensiva) baseou-se na alta integração e interdependência desses serviços, tornando recomendável sua contratação em um único lote. Esse agrupamento proporciona:

- Maior integração e eficiência na execução dos serviços;
- Redução de atrasos e retrabalho devido a diferenças metodológicas entre múltiplas empresas;
- Mitigação da retenção de conhecimento e da dependência excessiva de profissionais de diferentes fornecedores;
- Melhor aproveitamento de recursos e ganho em eficiência operacional;
- Centralização da gestão dos processos de segurança, facilitando a tomada de decisões e a implementação de melhorias contínuas.

A escolha de um lote único para os serviços de Segurança Defensiva também traz vantagens econômicas, evitando custos adicionais decorrentes da fragmentação dos serviços e facilitando a gestão integrada da segurança da informação na ANAC. Além disso, um fornecedor único pode oferecer um serviço mais coeso e alinhado com as necessidades específicas do órgão.

No que se refere às soluções exigidas para os itens 5 (Monitoramento e correlação de eventos de segurança da informação) e 8 (Solução de gerenciamento de vulnerabilidades de segurança), a empresa responsável pelo serviço de SOC poderá selecionar fornecedores de sua preferência, desde que atenda aos requisitos do Termo de Referência. Esse documento foi elaborado visando garantir ampla competitividade entre empresas do setor.

É importante destacar que o agrupamento proposto não compromete a competitividade do certame. O mercado conta com diversas empresas aptas a fornecer todos os itens do Lote 1, permitindo atender às necessidades da ANAC com maior eficiência técnica e econômica.

4. Requisitos da contratação

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Monitoramento contínuo da segurança dos sistemas e ativos de rede.
4.1.2. Centralização de logs em ferramenta específica e manutenção contínua desta.
4.1.3. Tratamento e resposta a incidentes de segurança da informação.
4.1.4. Gestão de vulnerabilidades em ferramenta específica, e manutenção contínua desta.
4.1.5. Pentest em aplicações, sistemas e ativos de rede da ANAC.
4.1.6. Apoiar técnica e operacionalmente a elaboração de normas e procedimentos na área de Segurança da Informação.
4.1.7. Reduzir riscos associados a perda de dados, comprometimento dos sistemas, imagem institucional deste órgão.

4.1.8. Melhorar a assertividade nos investimentos em soluções de segurança da informação efetivamente necessárias.
4.1.9. Reduzir os riscos associados aos ativos críticos.
4.1.10. Aumentar a maturidade de segurança da informação.
4.1.11. Desenvolver relatórios e apurações especiais, painéis gerenciais para apoio à tomada de decisão dos gestores, quanto ao risco da instituição.
4.1.12. Garantir a segurança da informação e comunicação no âmbito da ANAC e o sigilo das informações dos cidadãos.

4.2. Requisitos de Capacitação

4.2.1. Considerando-se as tecnologias disponíveis no ambiente de Tecnologia da Informação da ANAC, verifica-se que, para a execução do objeto dessa pretensa contratação, a empresa a ser contratada deverá dispor de Equipe Técnica especializada e com treinamento e capacitação atualizados nas tecnologias em questão.
4.2.2. Os requisitos de capacitação devem refletir os aspectos de monitoramento da segurança utilizando as principais metodologias, tecnologias, produtos e ferramentas que representem maior abrangência para os serviços de TI e soluções de infraestrutura de TI utilizados na ANAC.
4.2.3. Entre as principais tecnologias utilizadas, estão: Next Generation Firewall, Proteção a DDoS, IPS (Intrusion Prevention System), Balanceamento de Carga, WAF (Web Application Firewall), Web Gateway (Proxy), Mail Gateway (AntiSpam), Endpoint Security (Antivírus), DNS, Solução de SMTP, Solução de Next Generation AntiMalware, Solução de 2º Fator de Autenticação, VPN (Virtual Private Networks).

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, Portaria SGD/MGI nº 1.070, de 1º de junho de 2023 e outras legislações aplicáveis.
4.3.2. Política de Segurança da Informação no âmbito da Agência Nacional de Aviação Civil - ANAC, aprovada pela Instrução Normativa nº 128, de 6 de novembro de 2018.

4.4. Requisitos de Manutenção

4.4.1. Devido às características da solução, há necessidade de realização de manutenções preventivas, corretivas e evolutivas pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades.
4.4.2. Os serviços a serem prestados deverão ter garantia por todo o período do contrato.
4.4.3. A CONTRATADA deve assegurar e responsabilizar-se pela continuidade do fornecimento dos serviços contratados, zelando por sua disponibilidade e pela aderência aos requisitos de qualidade e aos Níveis Mínimos de Serviços Exigidos – o que inclui a necessidade de cumprir tempos de resposta a incidentes e de soluções de problemas nos ambientes gerenciados.
4.4.4. A CONTRATADA também responderá pela reparação dos danos causados à CONTRATANTE ou a TERCEIROS devido aos defeitos nos serviços ocasionados em razão de ação sua ação ou omissão.
4.4.5. Tratando-se de prestação de serviços, caso seja necessário substituir licenças equivalentes durante a vigência do Contrato, isso deverá ocorrer sem qualquer ônus para a ANAC.
4.4.6. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para a ANAC.
4.4.7. A ANAC somente autorizará que a CONTRATADA faça inventários nos equipamentos/serviços/softwares quando solicitado formalmente.
4.4.8. Cada novo release, versão de firmware, atualização de produtos que sejam relacionados aos itens do objeto deverá ser disponibilizada pela CONTRATADA sem ônus adicional.
4.4.9. A CONTRATADA garante que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets, devendo a CONTRATADA se responsabilizar por quaisquer despesas relacionadas que ocorram. Todos os serviços serão prestados esperando-se a aplicação das melhores práticas e recomendações do mercado e do Fabricante.
4.4.10. Somente serão aceitas justificativas para o não atendimento a um chamado técnico em tempo hábil, caso o fato seja gerado por motivo de força maior ou por dependência da ANAC, a CONTRATADA deve formalizar ao Gestor do Contrato ou ao Fiscal Técnico os motivos que impedem/impediram a execução do serviço.
4.4.11. Em nenhuma hipótese a CONTRATADA poderá se eximir do atendimento de um chamado sem que apresente justificativa técnica com os motivos que impedem a execução dos serviços.
4.4.12. A CONTRATADA é responsável pela manutenção preventiva, corretiva e evolutiva nos ativos de segurança que estão sob seus cuidados, devendo planejar e registrar o pedido de mudança que deverá ser levado para comitê e aprovado para execução.
4.4.13. Caso o técnico da CONTRATADA enseje dano irreparável aos equipamentos(s), ou sistema(s) ou dado(s) da Agência, por conta de conduta antiprofissional, erro ou quaisquer outros motivos, fica a CONTRATADA obrigada a realizar a troca por equipamento igual ou superior ao que foi danificado ou a normalização do sistema afetado.
4.4.14. Os serviços deverão ser devidamente licenciados, nos casos aplicáveis, para uso na ANAC durante a vigência do contrato.

4.4.15. Não deverão constar, quando aplicável, em listas dos respectivos fabricantes que indiquem que não serão mais desenvolvidos, atualizados, suportados ou comercializados durante a vigência do contrato.
4.4.16. É dever da CONTRATADA, em sua eventual necessidade de fornecimento de hardware visando adequada execução do contrato, instalar e manter esse hardware (inclusive nos aspectos de atualização e evolução).
4.4.17. Os serviços de atendimento à garantia deverão estar disponíveis em regime 24x7x365.
4.4.18. Deverão ser informados à CONTRATANTE os contatos para atendimento da garantia e manutenção, a serem prestados por meio dos canais: central de atendimento 0800, e-mail e presencial (caso o problema não possa ser resolvido por meio eletrônico), na modalidade "24x7", ou seja, 24 horas por dia, sete dias por semana, incluindo-se feriados.
4.4.19. Para garantia da qualidade de atendimento a central de atendimento deverá permitir acesso 24 horas ao Portal de Garantia Web, onde o cliente, no mínimo, possa rapidamente:
4.4.19.1 Abrir chamados de atendimento em garantia.
4.4.19.2 Receber numeração de forma automática. e
4.4.19.3 Acompanhar o andamento do chamado.

4.5. Requisitos Temporais
4.5.1. Os serviços devem ser prestados no prazo máximo de execução especificado na Ordem de Serviço (OS) emitida pela Contratante.
4.5.2. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.
4.5.3. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.
4.5.4. A Contratada deverá cumprir os prazos previstos neste Termo de Referência e atender às metas de tempo para execução das demandas conforme Níveis Mínimos de Serviço estabelecidos.

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 CONTRATANTE, e as partes se comprometem-se em cumprir suas obrigações, quando houver tratamento de dados pessoais, no que couber, ao abrigo da Lei nº 13.709, de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
4.6.2. A Contratada deverá atender aos requisitos de segurança previstos no framework de segurança, elaborado pela Secretaria de Governo Digital (SGD/MGI) e disponível em:
https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf
4.6.3. Sempre que solicitado pela CONTRATANTE, a CONTRATADA deverá apresentar, no prazo solicitado ou acordado, resguardados aspectos de confidencialidade, documentos comprobatórios referentes à estruturação de segurança e privacidade no contexto ao qual a Solução de TIC se insere, como:
a) Política de Segurança da Informação.
b) Relatório de Análise de Impacto à Proteção de Dados Pessoais.
c) Política de Backup.
d) Processo de Gestão Riscos da Solução de TIC.
e) Processo de Gestão de Incidentes.
f) Política de Controle de Acesso.
g) Plano de Continuidade Operacional e um Plano de Contingência.
h) Documento de Arquitetura Física e Lógica da Solução de TIC, entre outros relacionados com o tema da contratação.
4.6.4. A CONTRATADA deverá possuir Política de Segurança da Informação vigente e atualizada, possuindo ainda processo de revisão periódico formalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança da informação para assegurar a consistência, a privacidade e a confiabilidade dos dados e informações que serão tratados pela Solução de TIC
4.6.5. Em caso da ocorrência de incidentes de segurança, a CONTRATADA deverá observar e seguir todas as orientações da NC21/IN01/DSIC/SCS/GSIPR, homologada por meio da Portaria nº 40, de 8 de outubro de 2014.
4.6.6. Executar os serviços em conformidade com a legislação aplicável, em especial as certificações sobre segurança da informação solicitadas para Qualificação Técnica, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
4.6.7. Em caso de utilização de solução de nuvem pública, a CONTRATADA deverá seguir todas as orientações da Instrução Normativa nº 5 de agosto de 2021 do Gabinete de Segurança Institucional da Presidência da República, homologada por meio da Portaria nº 9, de 15 de março de 2018.
4.6.8. Mantendo-se a aplicação das normas vigentes, a CONTRATADA comprometer-se-á a preservar os dados da CONTRATANTE contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente à CONTRATANTE qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados.
4.6.9. Os dados, metadados, informações e conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos do previsto nesse Termo de Referência, sob nenhuma hipótese, sem autorização formal da CONTRATANTE.
4.6.10. A CONTRATADA deverá assinar Termo de Confidencialidade, resguardando que os recursos, dados e informações de propriedade da CONTRATANTE, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, constituam

informação privilegiada e possuem caráter confidencialidade.
4.6.11. A CONTRATADA deverá credenciar seus profissionais junto à ANAC, caso seja necessário o acesso às instalações para prestação dos serviços. Os prestadores de serviço, nas dependências da ANAC devem estar devidamente identificados por meio de crachá funcional ou equivalente.
4.6.12. Deve-se identificar qualquer equipamento da CONTRATADA que venha a ser instalado nas dependências da Agência, utilizando placas de controle patrimonial, selos de segurança etc.
4.6.13. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca da prestação do serviço, sem prévia autorização.
4.6.14. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo de informação de propriedade da CONTRATANTE, sem autorização.
4.6.15. A gerência da solução de segurança deve ser realizada com acesso protegido por senha.
4.6.16. Garantir a segurança das informações da CONTRATANTE e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido ou tido ciência no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.
4.6.17. Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação da ANAC.
4.6.18. A CONTRATADA deverá adotar controles e métodos presentes nas normas da família ISO 27000.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Aos profissionais da Contratada, quando nas dependências da ANAC, caberá:
4.7.1.1. Agir de maneira ética e profissional.
4.7.1.2. Manter conduta compatível com a moralidade administrativa.
4.7.1.3. Respeitar a capacidade e as limitações individuais de todos os usuários, sem qualquer espécie de preconceito ou distinção de raça, sexo, nacionalidade, cor, idade, religião, cunho político e posição social, abstendo-se, dessa forma, de causar-lhes dano moral.
4.7.1.4. Usar racionalmente os recursos e equipamentos de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos no desempenho de suas atribuições.
4.7.1.5. Estar devidamente identificado com crachá da empresa.
4.7.2. A contratação em questão trata-se de serviço continuado por alocação de profissionais especializados para atendimento à demanda contínua de monitoramento da segurança da informação da ANAC, portanto, os critérios e requisitos de sustentabilidade ambiental não são aplicáveis.
4.7.3. A CONTRATADA deverá realizar o serviço objeto deste Termo de Referência de forma completa, com atendimento a todos os requisitos presentes, sem que haja a necessidade de a ANAC realizar quaisquer contratações adicionais.
4.7.4. O horário de funcionamento da ANAC compreende o período das 8 (oito) às 18 (dezoito) horas, de segunda-feira a sexta-feira.

4.8. Requisitos da Arquitetura Tecnológica

4.8.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.
4.8.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.
4.8.3. Os serviços gerenciados de segurança devem ser executados por meio de Centro de Operações de Segurança, próprio da CONTRATADA, sendo localizado obrigatoriamente no Brasil.
4.8.4. O centro deve atender os requisitos mínimos, a saber:
4.8.4.1. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA, e cujas imagens possam ser recuperadas.
4.8.4.2. Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias.
4.8.4.3. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operações de Segurança.
4.8.4.4. Possuir solução de monitoramento de disponibilidade e desempenho.
4.8.4.5. O perímetro físico do Centro de operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido.
4.8.4.6. Ser vigiado de forma ininterrupta por segurança física especializada, armada (com utilização de arma de fogo), em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.
4.8.4.7. Ter controle de acesso físico com pelo menos 02 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura digital ou análise de retina.
4.8.4.8. Funcionar em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.
4.8.4.9. Possuir registro de entrada e saída de pessoas, mantido por pelo menos 90 (noventa) dias.
4.8.4.10. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.
4.8.4.11. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos

serviços contratados por, no mínimo, durante todo o período de vigência contratual.
4.8.4.12. Ser configurado de forma que a falha de um dos equipamentos, isoladamente, NÃO interrompa a prestação dos serviços.
4.8.4.13. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs - Uninterruptible Power Supply, para garantir a transição entre o fornecimento normal da energia e o grupo gerador.

4.8.4.13.1. Caso a CONTRATADA comprovadamente possua SOCs físicos de forma redundante, a CONTRATADA poderá garantir a continuidade do serviço com a disponibilização de, no mínimo, um sistema de energia ininterrupta, como um grupo gerador ou UPS, em cada localidade.
4.8.4.14. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.
4.8.4.15. Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores, estejam inacessíveis a leituras e a capturas externas desautorizadas.
4.8.4.16. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da CONTRATANTE, sem que haja impacto na operação do Centro de Operações de Segurança ou da própria CONTRATANTE.
4.8.5. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança.
4.8.6. Possuir nativamente solução de SecOps para uma colaboração entre a segurança e as operações de TI para minimizar os riscos de modo eficaz e para gerenciamento de incidentes de segurança da informação.
4.8.7. Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001 e Lei Geral de Proteção de Dados. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento, além de comprovadamente contar com um comitê responsável pelos controles e adequações.
4.8.8. A CONTRATADA será a responsável por fornecer todas as ferramentas e licenças para a prestação do serviço, exceto quando explicitamente definido.
4.8.9. A relação de ativos e serviços em operação na ANAC está disponível no Anexo I – Especificações Técnicas dos Serviços.
4.8.10. Com relação ao CTI, toda infraestrutura necessária para correta execução das atividades, como o ambiente computacional com alta disponibilidade, será de responsabilidade e deverá ser provida pela CONTRATADA.
4.8.11. A CONTRATADA responsável pelo serviço de CTI deverá prover plataforma para acesso pela ANAC às informações coletadas.

4.9. Requisitos de Projeto e de Implementação

4.9.1. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:
4.9.1.1. A CONTRATADA deverá desenvolver e apresentar macro cronograma de implantação e disponibilização dos serviços, além de definir estratégia de implantação, em conjunto com a equipe técnica da ANAC.
4.9.1.2. A ANAC deverá fornecer previamente à CONTRATADA responsável pelo serviço de CTI a lista de ativos de informação a serem monitorados.

4.10. Requisitos de Implantação

4.10.1. Tendo em vista que a presente contratação diz respeito à contratação de serviços, a CONTRATADA, no que couber, será responsável pela implantação/disponibilização da solução contratada.
4.10.2. A CONTRATADA deve formar os membros da equipe com perfil adequado aos Requisitos, antes do início da prestação do Serviço.
4.10.3. Os Serviços Especializados deverão ser prestados diretamente pela empresa CONTRATADA, sendo permitida a subcontratação apenas nos casos descritos no item 4.21.
4.10.4. A CONTRATADA deverá apresentar o plano de execução dos serviços contendo o detalhamento das ações necessárias para absorção dos conhecimentos e ativação dos serviços, bem como o estabelecimento da VPN entre os ambientes.
4.10.5. As responsabilidades e limites de atuação das equipes técnicas da CONTRATADA e da ANAC deverão observar o disposto no item 4.24.3. Vale atentar que a atividade referente à montagem do ambiente tecnológico é de responsabilidade da equipe técnica da CONTRATADA, ficando a cargo da ANAC a passagem de informações e concessões iniciais de acesso.

4.11. Requisitos de Garantia e Manutenção

4.11.1. A Contratada garantirá a disponibilização dos serviços prestados durante toda a vigência do Contrato. Nesse período a Contratada se obriga a corrigir quaisquer defeitos nos serviços executados, exceto se o defeito estiver vinculado a ferramentas opensource. Os defeitos compreendem, mas não se limitam a imperfeições percebidas num serviço contratado, ausência de artefatos obrigatórios e qualquer outra ocorrência que impeça o andamento normal dos serviços contratados..
4.11.2. Os serviços a serem prestados deverão ter garantia por todo o período do contrato.
4.11.3. Caberá à Contratada, durante toda a vigência do Contrato, e por 90 (noventa) dias após o seu término, realizar todas as correções decorrentes dos erros ou falhas cometidas na execução dos serviços contratados e/ou decorrentes de integração e adequação da solução, desde que, comprovadamente, não tenham se dado em razão das especificações feitas pela

CONTRATANTE.
4.11.4. As glosas decorrentes de demandas em garantia abertas no período supracitado de 90 (noventa) dia subsequentes ao término do contrato poderão ser aplicadas às faturas ainda não liquidadas ou da caução apresentada como garantia pela Contratada.
4.11.5. Todos os softwares utilizados nos itens 5 e 8 do Grupo 1 (Tabela 1.1) para a prestação de serviço devem estar licenciados contemplando atualizações e garantia total por todo o período de vigência do contrato, caso haja renovação do contrato será também renovada a garantia, conforme quantidades, requisitos e especificações constantes deste documento.

4.12. Requisitos de Experiência Profissional
4.12.1. Os serviços de assistência técnica, suporte, garantia, atualizações, instalações e outros deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

4.13. Requisitos de Formação da Equipe
4.13.1. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos no Anexo I – Especificações Técnicas dos Serviços.

4.14. Requisitos de Metodologia de Trabalho
4.14.1. A execução dos serviços está condicionada ao recebimento pela Contratada de Ordem de Serviço (OS) emitida pela Contratante.
4.14.2. A OS indicará o serviço, a quantidade e a localidade na qual deverão ser prestados.
4.14.3. As Ordens de Serviços deverão ser classificadas pela CONTRATANTE, conforme nível e continuidade de execução:
4.14.3.1. Rotineira: atividades contínuas, realizáveis periodicamente, emitidas para execução durante a vigência do contrato. Podendo, mediante realinhamento, ter novas atividades inseridas ou excluídas no decorrer da vigência contratual.
4.14.3.2. Exclusiva: atividades de natureza não contínua, emitidas a partir da demanda da CONTRATANTE.
4.14.4. A Contratada deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7(sete) dias por semana de maneira eletrônica e de segunda a sexta-feira, em dias úteis, das 8 (oito) às 18 (dezoito) horas, por via telefônica.
4.14.5. Para o Grupo 1, a CONTRATADA deverá disponibilizar 04 (quatro) tipos de canais de comunicação, a saber:

Tabela 4.1

Grupo de Tecnologia	Classificação
Linha de telefonia gratuita (0800) de cobertura nacional	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 3
Portal interno, com possibilidade de interação não humana com os chamados (*chatbot*)	Tipo 4

4.14.6. Independente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM (do inglês Information Technology Service Management - Gerenciamento de Serviços de TI). Ou seja, imaginando que a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.
4.14.7. Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.
4.14.8. Sobre o canal de comunicação tipo 3: Quando ocorrer um incidente, os chamados deverão ser abertos de forma

automática, por meio do SOC da CONTRATADA, para que assim, os SLAs estabelecidos sejam alcançados
4.14.9. Para um eventual cenário de crise, ou seja, onde o negócio fim da CONTRATANTE estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.
4.14.10. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo TLS (do inglês Secure Socket Layer) A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados ou armazenados.
4.14.11. A sala virtual ainda deve ter capacidade para minimamente 10 (dez) pessoas da CONTRATANTE simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.
4.14.12. A execução do serviço dever ser acompanhada pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

4.14.13. Para assegurar a governança adequada em relação ao modo de atuação da área de TIC na entrega de serviços relacionados aos itens 9 (Segurança de Redes) e 10 (Segurança de Aplicação), a CONTRATADA deverá:

4.14.13.1 Implementar as seguintes práticas:

a) Gerenciamento de requisição de serviços;

b) Gerenciamento de mudanças;

c) Gerenciamento de problemas; e

d) Gerenciamento de incidentes.

4.14.13.2 Observar que as soluções técnicas aplicadas na execução dos serviços deverão ser posteriormente analisadas e registradas, quando necessário, pela CONTRATADA
na base de conhecimentos da solução de ITSM, de modo a proporcionar maior eficiência nos próximos atendiment

4.14.14. Para os serviços dos Grupos 2 e 3, a(s) CONTRATADA(S) deverão fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e de segunda a sexta-feira, em dias úteis, das 8 (oito) às 18 (dezoito) horas, por via telefônica.
4.14.15. Os chamados para atendimento da(s) CONTRATADA(s) poderão ser abertos apenas pelos contatos autorizados pela equipe técnica da CONTRATANTE.
4.14.16. Os serviços de inteligência de ameaças cibernéticas (CTI) devem ser prestados em regime 24x7x365 no formato de Software as a Service (SaaS).

4.14.17. Os serviços de teste de invasão (Pentest) serão prestados sob demanda.

4.15. Requisitos de Segurança da Informação e Privacidade
4.15.1. A CONTRATADA deverá se comprometer e cumprir ao exigido pela Política de Segurança da Informação no âmbito da Agência Nacional de Aviação Civil - ANAC, aprovada pela Instrução Normativa nº 128, de 6 de novembro de 2018 e suas normas complementares.
4.15.2. A CONTRATADA deverá garantir a segurança das informações da ANAC e se compromete a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.
4.15.3. Deverá ser celebrado TERMO DE COMPROMISSO DE MANUTENÇÃO E SIGILO entre a CONTRATADA e a CONTRATANTE para garantir a segurança das informações da ANAC.
4.15.4. A CONTRATADA, após a assinatura do contrato, por meio de seu representante, assinará TERMO DE COMPROMISSO DE MANUTENÇÃO E SIGILO em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.
4.15.5. Além do termo citado, a CONTRATADA deverá apresentar para cada funcionário que vier a executar atividades referentes ao objeto da contratação, TERMO DE CIÊNCIA em que seus profissionais declaram estar cientes das responsabilidades pela manutenção de sigilo e confidencialidade.
4.15.6. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, e suas alterações pela Lei nº 13.852/2019 que entrou em vigor no final de setembro de 2020, juntamente com as penalidades que entraram em vigor em agosto de 2021.
4.15.7. A CONTRATADA deverá atender à legislação, principalmente à Instrução Normativa GSI/PR nº 05, de 30 de junho de 2021, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina acerca dos requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
4.15.8. A CONTRATADA deverá fornecer link de comunicação dedicado, próprio, com acesso restrito e criptografado, para

conectar o Datacenter da CONTRATANTE (localizado no Centro de Treinamento da ANAC) ao SOC ou à nuvem da CONTRATADA.
4.15.9. Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com links xDSL (Digital Subscriber Line) Também a fim de garantir a disponibilidade da conexão, deverá a CONTRATADA garantir que tal conexão esteja protegida contra-ataques de DDoS - Distributed Denial of Service.
4.15.10. Em qualquer que seja o tipo de conexão, será de responsabilidade da CONTRATADA, a contratação junto as devidas operadoras, bem como seus devidos custos durante todo o período de vigência do contrato.
4.15.11. A fim de garantir a segurança do tráfego bidirecional entre a CONTRATANTE e o Centro de Operações de Segurança da CONTRATADA, as conexões devem ser criptografadas, ou seja, a CONTRATADA deverá estabelecer VPN's do tipo site to site.
4.15.12. A fim de garantir a segurança entre a CONTRATANTE e os Centro de Operações de Segurança da CONTRATADA, não será permitido Centro de Operações de Segurança terceirizado ou consórcio de CONTRATANTES. A CONTRATADA deve ter e manter Centros de Operações de Segurança próprios.
4.15.13. Será de responsabilidade e propriedade da CONTRATADA as soluções para estabelecer as VPNs entre os firewalls da CONTRATADA e CONTRATANTE. Se necessário, caberá à CONTRATANTE apenas a disponibilidade de infraestrutura física no seu Data Center, infraestrutura física leia-se: energia elétrica, espaço no rack, climatização adequada, e sistemas de combate a incêndio. Tais equipamentos e/ou soluções devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.
4.15.14. Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATANTE, empregadas na prestação de serviços à CONTRATANTE, bem como solicitar a revogação destas à CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.
4.15.15. Tais exigências visam proteger a CONTRATANTE contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

4.16. Vistoria

4.16.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, no horário das 10h às 16h.
4.16.2. Os licitantes poderão solicitar o agendamento da vistoria pelo telefone (61) 3314-4213 ou pelo e-mail std@ANAC.gov.br, cujo campo "assunto" da mensagem deverá conter o texto "Vistoria – Edital X/2024" com no mínimo 48 horas úteis de antecedência
4.16.3. Os licitantes serão comunicados, por e-mail, dos momentos e locais onde devem se apresentar para a vistoria. É de responsabilidade do licitante a correta prestação de informações para a comunicação deste evento, não obrigando a ANAC a sanar qualquer falha, mesmo que conhecida, na prestação destas informações
4.16.4. Os custos da vistoria são de responsabilidade do licitante, incluindo seus deslocamentos em veículo próprio aos locais vistoriados
4.16.5. Os licitantes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a vistoria, simples participação na vistoria caracteriza o compromisso irretratável de guarda do sigilo dos dados colhidos.
4.16.6. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.
4.16.7. Para a vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.
4.16.8. Ao término da vistoria será emitido, em 2 (duas) vias, o termo de Declaração de Vistoria.
4.16.9. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes. A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
4.16.10. Caso decida pela não realização da vistoria, o licitante deverá apresentar a Declaração de responsabilidade de não vistoriar, conforme o ANEXO X - DECLARAÇÃO DE RESPONSABILIDADE DE NÃO VISTORIA deste Termo de Referência, juntamente com os documentos de habilitação.
4.16.11. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.17. Outros Requisitos Aplicáveis

4.17.1. Não se aplica.

4.18. Sustentabilidade

4.18.1. O objeto deste TR não apresenta especificidades para aplicação de requisitos relacionados a critérios e práticas de sustentabilidade.

4.19. Da vedação de utilização de marca/produto na execução do serviço
4.19.1. Não se identificou a necessidade de vedação do emprego de marcas ou produtos de bens empregados na execução dos serviços.

4.20. Da exigência de carta de solidariedade
4.20.1. Não se aplica.

4.21. Subcontratação
4.21.1. Não é admitida a subcontratação do objeto contratual, exceto para a prestação de serviços de "remote hands", relacionados ao item 9 do Grupo 1, Segurança de Redes, para atividades que demandem intervenção presencial, como acompanhamento presencial de fornecedor de suporte, manutenções de equipamentos, substituição de peças, etc.

4.21.2. Justificativa da subcontratação

4.21.2.1. A prestação do serviço "Segurança de Redes" contempla, entre outras atividades, a operação dos equipamentos de segurança da informação instalados nas unidades da Anac localizadas em Brasília/DF, São Paulo/SP, São José dos Campos/SP e Rio de Janeiro/RJ.

O endereço das unidades está disponível no link:
https://www.gov.br/anac/pt-br/acesso-a-informacao/institucional/enderecos-e-telefones

4.21.2.2. A operação desses ativos é realizada, majoritariamente de forma remota, não exigindo a presença local de profissionais para seu funcionamento. Porém, em determinadas situações pontuais, como manutenção do equipamento ou substituição de peças, faz-se necessário o acompanhamento presencial por profissional capacitado.

4.21.2.3. Historicamente, tais intervenções acontecem com baixa frequência, não justificando a manutenção de um profissional na localidade. Além disso, a não previsão da subcontratação para os casos mencionados restringiria consideravelmente a participação das empresas na licitação, já que poucas dispõem de profissionais em todas as localidades citadas. Dessa forma, haveria grandes prejuízos ao princípio da competitividade, princípio explicitamente previsto na legislação licitatória.

4.21.2.4. Não obstante, cabe ressaltar que a Anac também não dispõe de servidores capacitados para o acompanhamento dessas atividades nas localidades de São Paulo, São José dos Campos e Rio de Janeiro.

4.21.2.5. Dessa forma, faz-se necessária a previsão dessa exceção para serviços de "remote hands", de forma a propiciar a ampla competitividade da licitação e também o menor custo operacional do contrato.

4.22. Da verificação de amostra do objeto
4.22.1. Não se aplica.

4.23. Garantia da Contratação
4.23.1. Será exigida a garantia da contratação de que tratam os arts 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.
4.23.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato
4.23.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.
4.23.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.24. Informações relevantes para o dimensionamento ou apresentação da proposta
4.24.1. A demanda da ANAC está descrita ao longo deste Termo de Referência.

4.24.2. O Anexo IX contém o modelo de apresentação da proposta comercial e a planilha de custos e formação de preços que deve ser entregue pelas empresas licitantes durante a fase de seleção do fornecedor.

4.24.3. Os serviços de Service Desk (com suporte de atendimento remoto e presencial) para usuários, monitoração de ambiente tecnológico (NOC - Network Operations Center) e operação da infraestrutura de TIC da ANAC são atualmente prestados pela empresa GLOBAL WEB OUTSOURCING DO BRASIL S.A, através do contrato 21/2021.

4.24.4. No advento da presente licitação, a empresa que se sagrar vencedora do Grupo 1 passará a ser responsável pela operação da infraestrutura de segurança da ANAC (conforme Anexo II - Ambiente Tecnológico), mantendo-se sob responsabilidade da Global WEB os demais serviços listados no contrato 21/2021, conforme tabelas abaixo:

Tabela 4.2

SERVIÇO	RESPONSÁVEL
ATENDIMENTO DE SERVICE DESK – Modalidade REMOTO	Global WEB - Contrato 21/2021
ATENDIMENTO DE SERVICE DESK – Modalidade PRESENCIAL	Global WEB - Contrato 21/2021
Apoio ao Processo de Excelência no Atendimento	Global WEB - Contrato 21/2021
Apoio ao Planejamento e a Gestão de Serviços de TIC	Global WEB - Contrato 21/2021
Apoio à Gestão do Conhecimento e Documentação de TI	Global WEB - Contrato 21/2021
Suporte a Redes locais, MAN, WAN e SD-WAN	Global WEB - Contrato 21/2021
Suporte a Telefonia VoIP e Videoconferência	Global WEB - Contrato 21/2021
Suporte a Ambientes de Data Center e Sistemas Operacionais	Global WEB - Contrato 21/2021
Suporte ao Armazenamento de Dados e Backup	Global WEB - Contrato 21/2021
Suporte ao Ambiente Colaborativo	Global WEB - Contrato 21/2021
Suporte a Deploy e Produção de Aplicações Corporativas	Global WEB - Contrato 21/2021
Suporte a Deploy e Produção de Aplicações de Mercado	Global WEB - Contrato 21/2021
Suporte a Orquestração e Automação de Aplicações	Global WEB - Contrato 21/2021
Suporte à Administração de Banco de Dados	Global WEB - Contrato 21/2021
Suporte à Ferramentas de Tratamento e Análise de Dados	Global WEB - Contrato 21/2021
Suporte a Monitoração de Serviços de TI	Global WEB - Contrato 21/2021
MONITORAÇÃO DE AMBIENTE TECNOLÓGICO (NOC)	Global WEB - Contrato 21/2021

SERVIÇO	RESPONSÁVEL
Operação da infraestrutura de segurança	Empresa vencedora do Grupo 1 da presente licitação

4.24.5. Para a contratação do serviço de CTI, a quantidade estimada e os respectivos ativos de informação a serem monitorados, são os seguintes:

Tabela 4.3

ITEM	DESCRIÇÃO	ATIVOS	QTD
1	Monitoração da surface web, deep web, e dark web	Pessoas de Interesse	40
2	Monitoração da surface web, deep web, e dark web	Produtos/Marcas	15
3	Sites e contas fraudulentas	Takedown por Ano	120
4	Monitoração de fontes de informações	Domínios/subdomínios	60
5	Monitoração de vazamento de informações	Nomes de Empresas Fornecedoras	25

4.24.6. Os serviços de teste de invasão serão realizados sob demanda, considerando as quantidades máximas listadas na tabela abaixo, para o período de 24 meses:

Tabela 4.4

ITEM	SERVIÇO	QTD
1	Realizar Teste de Invasão (Pentest) - Externo	24
2	Realizar Teste de Invasão (Pentest) - Interno	24
3	Realizar Teste de Invasão (Pentest) - Aplicação Web	24
4	Realizar Teste de Invasão (Pentest) - API	24
5	Realizar Teste de Invasão (Pentest) - Aplicativo Móvel	16
6	Realizar Teste de Invasão (Pentest) - Redes sem fio	4
7	Realizar Teste de Invasão (Pentest) - Engenharia Social	8
8	Realizar Teste de Invasão (Pentest) - Redes	12
9		12

	Realizar Teste de Invasão (Pentest) - Nuvem	
10	Realizar Teste de Invasão (Pentest) - Máquina do Usuário	12
11	Realizar Teste de Invasão (Pentest) - Ransomware	24
12	Realizar Teste de Invasão (Pentest) - Banco de Dados	24
13	Realizar Teste de Invasão (Pentest) - Acesso Remoto	24
14	Realizar Teste de Invasão (Pentest) - Phishing	4
15	Realizar Teste de Invasão (Pentest) - Física	4

4.24.7. Nas situações em que há necessidade de cobertura em regime 24/7 deve-se dimensionar uma quantidade de profissionais adequada à cobertura dos turnos, respeitando-se os limites de carga horária previstos na legislação.

5. Modelo de execução do objeto

5. MODELO DE EXECUÇÃO DO OBJETO

Dado o caráter inédito da prestação dos serviços referenciados no objeto deste Termo de Referência e à consequente necessidade de ganho de maturidade pela equipe de fiscalização do contrato, entende-se razoável que a prestação dos serviços ocorra em fases, permitindo assim que os fiscais tenham melhor compreensão da execução prática dos serviços.
Nesse sentido, elencam-se os seguintes benefícios:

- Monitoramento contínuo: A divisão do serviço em fases possibilita um acompanhamento contínuo e detalhado de cada etapa, permitindo a identificação e correção de possíveis falhas ou desvios antes que se tornem problemas maiores.
- Ajustes e melhorias: Com a implementação faseada, é possível realizar ajustes e melhorias ao longo do processo, baseando-se no feedback e nas observações feitas durante cada fase. Isso assegura que o serviço final atenda plenamente às necessidades e expectativas da unidade.
- Capacitação da Equipe: A prestação em fases oferece à equipe a oportunidade de se familiarizar gradualmente com o novo serviço, adquirindo o conhecimento e as habilidades necessárias para uma fiscalização eficaz e eficiente.
- Redução de Riscos: A abordagem faseada minimiza os riscos associados à implementação de um serviço novo e desconhecido, permitindo uma gestão de riscos mais controlada e segura.

Conforme a execução dos serviços e o andamento dos contratos, os prazos referenciados nas tabelas 5.2 e 5.5 poderão ser antecipados, conforme acordo entre as partes.

5.1. Serviços gerenciados de segurança (Grupo 1)

5.1.1. Cronograma de realização dos serviços:

Tabela 5.1

Prazo	Evento	Responsável
D	Assinatura do contrato	ANAC e Contratada
Até D + 5	Reunião inicial	ANAC e Contratada
X (conforme tabela 5.2)	Apresentação do projeto executivo	Contratada
X+15	Avaliação do projeto executivo	ANAC
X + 60	Implantação dos serviços.	Contratada
X + 65	Emissão da Ordem de Serviço	

Conforme constar na Ordem de Serviço.	Início da execução dos serviços	Contratada

Tabela 5.2

Grupo	Item	Especificação	Valor de X
1	**1**	Apoio à Gestão de Segurança	Até D + 15
	2	Gestão de Ativos e Configuração Segura	Até D + 15
	3	Gestão de Conta, Controle de Acesso e Auditoria	Entre D + 120 e D + 135
	4	Gestão de incidentes de segurança da informação (Blue Team)	Até D + 15
	5	Monitoramento e correlação de eventos de segurança da informação	Até D + 15
	6	Serviço de contratação de pacotes adicionais de 500 EPS da ferramenta SIEM por 12 meses	Sob demanda
	7	Gestão de vulnerabilidades	Entre D + 120 e D + 135
	8	Solução de gerenciamento de vulnerabilidades de segurança	Entre D + 120 e D + 135
	9	Segurança de Redes	Entre D + 240 e D + 255
	10	Segurança de Aplicação	Entre D + 240 e D + 255

5.1.2. A CONTRATADA deverá atender às seguintes condições gerais para início da prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços, sem ônus adicionais à CONTRATANTE:

5.1.2.1. Reunião de início do projeto (kick-off), a ser realizada em até 5 (cinco) dias corridos após a assinatura do contrato, a ser previamente agendada pela CONTRATANTE. A reunião poderá ser remota ou presencial na Sede da CONTRATANTE.
5.1.2.2. Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança da CONTRATANTE já ativa e as soluçoes opensource que podem ser necessárias durante a vigência contratual, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para prévia aprovação pela CONTRATANTE.
5.1.2.3. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços.
5.1.2.4. A elaboração do Projeto Executivo é de responsabilidade da CONTRATADA, e deverá conter as fases do projeto, os cronogramas de execução, e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.
5.1.2.5. A conclusão da fase de implantação dos serviços é de até 90 (noventa) dias corridos, contados da data de assinatura do contrato, iniciando-se a fase de prestação mensal dos serviços, apenas após a emissão do termo de recebimento definitivo.
5.1.2.6. A implantação será considerada concluída quando todas as consoles estiverem implementadas.
5.1.2.7. O projeto executivo deve atender minimamente os seguintes requisitos:
5.1.2.7.1. Conter a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa.
5.1.2.7.2. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade da CONTRATANTE.
5.1.2.7.3. Para a implantação dos serviços, indicar de forma detalhada as condições de rollback de cada mudança no ambiente da CONTRATANTE.
5.1.2.7.4. Estimar o consumo de unidades de rack em U’s e de energia de cada ativo a ser instalado nas dependências da CONTRATANTE.
5.1.2.8. Os softwares e demais componentes necessários à correta prestação dos serviços deverão:
5.1.2.8.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da CONTRATANTE, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade.

5.1.2.8.2. Conter a última versão de software e firmware homologado pelo fabricante.
5.1.2.8.3. Ter configuradas senhas de acesso para que a equipe de funcionários designados pela CONTRATANTE efetue o acesso para a visualização das configurações e logs (acesso seguro e remoto).
5.1.2.8.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela CONTRATANTE em caso de emergência.

5.1.2.8.5. Para as soluções de software, a Anac poderá disponibilizar máquinas virtuais através de infraestrutura de virtualização MS Hyper-V 2019.
5.1.2.9. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 21h (vinte e uma horas) – além de finais de semana e feriados, conforme disponibilidade da CONTRATANTE.
5.1.2.10. Caso a CONTRATANTE encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências.
5.1.2.11. Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade na CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação, sem quaisquer custos adicionais a CONTRATANTE.
5.1.2.12. Para todos os componentes da solução, a CONTRATADA deverá implementar e documentar as respectivas configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.
5.1.2.13. Para o planejamento e o acompanhamento da instalação dos softwares necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as-built, e para as demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS
5.1.2.14. As qualificações técnicas mínimas exigidas para o perfil de GERENTE DE PROJETO da CONTRATADA são:

Tabela 5.3

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Conhecimento avançado em gerência de projetos, com experiência mínima de 12 (doze) meses.
Treinamentos/ Certificações	Ao menos uma das certificações de segurança da informação: • Project Management Professional (PMP). • Prince2 Practitioner Certificate in Projetct Management. • Professional Scrum Master I.

5.1.2.15. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais com perfil de GERENTE DE PROJETO, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme Tabela 5.3 de exigências de qualificações.
5.1.2.16. O planejamento dos serviços terá impacto direto no pagamento de acordo com as entregas.

5.1.3. Gestão de catálogo de serviços
5.1.3.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação da

CONTRATANTE, será definido em conjunto com a CONTRATADA uma lista de serviços que a CONTRATADA deverá ser capaz de entregar. Tal definição deverá ser aceita por ambas as partes e ficar disponível para consulta.
5.1.3.2. É de responsabilidade da CONTRATADA manter, atualizar, revisar, os serviços disponíveis para cada grupo de serviço. As responsabilidades da CONTRATANTE estão relacionadas a aprovação de um novo serviço, ou a aposentadoria de um ou mais serviços existentes.
5.1.3.3. O catálogo de serviço deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma on-line para a CONTRATANTE, onde ela poderá consultar a qualquer tempo os serviços disponíveis.
5.1.3.4. Apesar de já existir uma definição prévia de parte dos serviços a serem entregues pela CONTRATADA, incluídas no presente documento no Anexo III – Catálogo de Serviços, a CONTRATANTE a qualquer tempo poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço em comum acordo com a CONTRATADA.
5.1.3.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviço seja sugerida por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas a CONTRATANTE tal ação.

5.1.4. Rotinas a serem cumpridas
5.1.4.1. Portal de indicadores de serviços
5.1.4.2. Um portal de indicadores deverá ser disponibilizado à CONTRATANTE e deverá contemplar, no mínimo, os requisitos abaixo:
5.1.4.2.1. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (do inglês software as a service), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.
5.1.4.2.2. O portal deverá estar acessível a CONTRATADA via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia TLS 1.2 ou superior.
5.1.4.2.3. A CONTRATANTE terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.
5.1.4.2.4. Deverá disponibilizar para os usuários da CONTRATANTE, a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico estar disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.
5.1.4.2.5. O portal ainda deverá disponibilizar os seguintes modelos gráficos para os usuários:
5.1.4.2.5.1. Gráfico do tipo Pizza
5.1.4.2.5.2. Gráfico do tipo Barra
5.1.4.2.5.3. Gráfico do tipo linha
5.1.4.2.5.4. Gráfico do tipo área
5.1.4.2.5.5. Gráfico do tipo funil
5.1.4.2.5.6. Gráfico do tipo bolha
5.1.4.2.6. INDICADORES DE RISCO – KRI:
5.1.4.2.7. Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas.
5.1.4.2.8. O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e /ou baixa.
5.1.4.2.9. INDICADORES DE META E PERFORMANCE – KGI e KPI:
5.1.4.2.10. O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de Análise, contenção, erradicação e recuperação, possibilitando a filtragem deles por período:
5.1.4.2.11. Últimos 15 dias.
5.1.4.2.12. Últimos 30 dias.
5.1.4.2.13. Últimos 45 dias.
5.1.4.2.14. Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro de período filtrado, mostrando na linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.
5.1.4.2.15. Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (Análise, contenção, erradicação e recuperação).
5.1.4.2.16. INDICADORES POR CATEGORIA MITRE ATT&CK:
5.1.4.2.17. O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo:
5.1.4.2.17.1. Initial Access.
5.1.4.2.17.2. Execution.
5.1.4.2.17.3. Persistence.
5.1.4.2.17.4. Privilege Escalation.
5.1.4.2.17.5. Defense Evasion.
5.1.4.2.17.6. Lateral Movement.
5.1.4.2.17.7. Collection.

5.1.4.2.17.8. Command and Control.
5.1.4.2.17.9. Exfiltration.
5.1.4.2.17.10. Impact.
5.1.4.2.18. Todos os indicadores exibidos pelo portal, devem possuir a funcionalidade drill down, para que que os usuários possam criar novas visualizações e filtros dos dados exibidos
5.1.4.2.19. Todos os indicadores exibidos pelo portal, devem ainda possuir funcionalidade de exibição dos dados gerados do gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.
5.1.4.2.20. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos de tempo.
5.1.4.2.21. A qualquer tempo a CONTRATANTE poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado
5.1.4.2.22. Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time)
5.1.4.2.23. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo de nível de serviço definido no presente termo de referência.
5.1.4.2.24. Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e dashboards de todas as soluções que compõem o objeto.

5.1.5. Serviço de acompanhamento de entregas
5.1.6. Deverá ser provido um serviço de acompanhamento de entregas através de reunião para cadência do contrato de forma quinzenal.
5.1.6.1. Entregável: Ata de reunião
5.1.7. Deverá ser feito o acompanhamento periódico dos indicadores listados no contrato para antecipar desvios e corrigi-los antes que saiam das conformidades exigidas.
5.1.7.1. Entregável: Acompanhamento periódico a partir das ferramentas de registro de chamado ou medição (Portal de Indicadores).
5.1.8. Todos os entregáveis do contrato são acompanhados pelo SDM – desde SLA de atendimento à relatórios, a fim de garantir a conformidade e cadência correta estabelecida.
5.1.8.1. Entregável: Checklist periódico dos entregáveis do projeto, conforme Termo de Referência.
5.1.9. Deverá ser feito o acompanhamento do cronograma de faturamento mensal do contrato.
5.1.10. Deverá manter a matriz de comunicação atualizada dos dois lados do contrato – quem a CONTRATADA deve acionar e quem a CONTRATANTE deve acionar em casos específicos ou de escalação.
5.1.10.1. Entregável: Documento formal conforme formato pré-estabelecido.

5.1.11. Serviço de conformidade de desempenho contratual
5.1.12. Deve ser provido serviço de conformidade de desempenho do contrato no qual deverão ser providas reuniões mensais entre a CONTRATANTE e a CONTRATADA com intuito de validação da satisfação referente aos serviços prestados.
5.1.13. Estas reuniões devem servir para identificação das necessidades da CONTRATANTE onde deverão ser apontados problemas recorrentes ou pontuais que estejam impactando o a qualidade da execução do contrato.
5.1.14. Após essas reuniões deverão ser formulados planos de ações corretivos para cada área/serviço que não esteja cumprindo os padrões de qualidade exigidos no contrato.
5.1.15. O serviço deve ser executado por um especialista em resolução de crises ou temas críticos da CONTRATADA que funcione como moderador entre o time de entrega da CONTRATATADA com os gestores do contrato da CONTRATANTE.
5.1.16. Entende-se como CRISE, a atuação que é ou será baseada no desenvolvimento de um plano de ação, para temas que gerem ônus imediato à CONTRATANTE, ônus direto e imediato à CONTRATADA, risco de exposição do ambiente do cliente, risco de cancelamentos de contratos. Além disso, crises serão tratadas em conjunto com todas as áreas envolvidas, até a finalização do plano de ação de correção.
5.1.17. O especialista responsável por este serviço deve atuar também na escalação de temas não críticos, do dia a dia do contrato que não estejam sendo respondidos devidamente pela CONTRATADA.
5.1.18. Entende-se como ESCALAÇÃO, problemas diários de clientes em que a tratativa não foi eficaz e efetiva e/ou fora do tempo esperado/acordado, fazendo com que a CONTRATANTE eleve o tema para um nível hierárquico superior da CONTRATATADA. Exemplos:
5.1.18.1. Falta de atuação de algum time específico.
5.1.18.2. Falta de resposta à um e-mail, chamado, questionamentos do cliente.
5.1.18.3. Falta de solução à um problema sinalizado pelo cliente.
5.1.18.4. Chamado em aberto, não atendido dentro do SLA acordado em contrato.
5.1.18.5. Insatisfação do cliente sobre um entregável como relatório, boletins, atuação/ postura de recursos ou times.
5.1.19. Este serviço deverá prover ainda um indicador denominado NPS (Net Promoter Score) que consiga metrificar a satisfação da CONTRATANTE em relação aos serviços prestados que estejam estipulados no contratoEstá métrica deverá seguir os padrões e fórmulas comuns de mercado e deverá ser atualizada e apresentada mensalmente aos gestores do contrato.

5.2. Serviços de inteligência de ameaças cibernéticas (Grupo 2)

5.2.1. Cronograma de realização dos serviços:

Tabela 5.4

Prazo	Evento	Responsável
D	Assinatura do contrato	ANAC e Contratada
Até D + 5	Reunião inicial	ANAC e Contratada
X (conforme tabela 5.5)	Apresentação do projeto executivo	Contratada
X+5	Avaliação do projeto executivo	ANAC
X + 15	Implantação dos serviços.	Contratada
X + 20	Emissão da Ordem de Serviço	
Conforme constar na Ordem de Serviço.	Início da execução dos serviços	Contratada

Tabela 5.5

Grupo	Item	Especificação	Valor de X
2	**11**	Inteligência de Ameaças Cibernéticas	Entre D + 120 e D + 135

5.3. Serviços de teste de invasão (Grupo 3)

5.3.1. Cronograma de realização dos serviços:

Tabela 5.6

Até	Evento	Responsável
D	Assinatura do contrato	ANAC e Contratada
D+5	Reunião inicial	ANAC e Contratada
D+15	Apresentação do plano de execução dos serviços	Contratada
D+20	Avaliação do plano de execução dos serviços	ANAC

Sob demanda	Emissão da ordem de serviços	ANAC

5.4. A emissão das ordens de serviço serão realizadas sob demanda, conforme conveniência e oportunidade da CONTRATANTE.
5.5. Documentação Mínima Exigida: a Contratada deverá disponibilizar mensalmente relatórios gerenciais que demonstrem a execução das atividades para que a equipe de fiscalização da ANAC possa atestar o provimento dos serviços.

5.6. Local e horário da prestação dos serviços
5.6.1. Os serviços dos Grupos 1 e 2 devem obrigatoriamente serem executados, ofertados, e estarem acessíveis a CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.
5.6.2. Os serviços do Grupo 3 serão executados sob demanda, de acordo com a emissão da Ordem de Serviço.
5.6.3. Todo o atendimento deve ser iniciado por profissionais da CONTRATADA, que estejam em horário de trabalho no momento do atendimento. Não sendo permitido o uso de funcionários no chamado “Regime de Plantão”, “Sobreaviso” e/ou sistemas similares, onde o funcionário apenas passa a trabalhar no momento do incidente.
5.6.4. A modalidade principal de atendimento será do tipo remota.
5.6.5. Para os itens 6 e 7 do Grupo 1, que envolvem a operação da infraestrutura de segurança da ANAC, a CONTRATADA deverá estar apta a deslocar a equipe para atendimento presencial em situações que assim o requeiram, como tratamento de incidentes, acompanhamento de manutenções pelo fabricante etc.
5.6.6. As unidades da ANAC que contam com equipamentos de segurança instalados são:

Tabela 5.6

Localidade	Equipamentos
Sede	2 firewalls de rede (cluster ativo/standby) + gerência da solução 2 firewalls de aplicação (cluster ativo/standby) + gerência da solução
Centro de Treinamento	2 firewalls de rede (cluster ativo/standby) 2 firewalls de aplicação (cluster ativo/standby)
Representação Regional Rio de Janeiro	2 firewalls de rede (cluster ativo/standby)
Representação Regional São José dos Campos	2 firewalls de rede (cluster ativo/standby)
Representação Regional São Paulo - RRSP	2 firewalls de rede (cluster ativo/standby)

5.6.7. Os endereços das unidades podem ser consultados no link:

https://www.gov.br/anac/pt-br/acesso-a-informacao/institucional/enderecos-e-telefones

5.7. Materiais a serem disponibilizados
5.7.1. Para a perfeita execução dos serviços, a CONTRATADA deverá disponibilizar os materiais, pessoas, equipamentos,

ferramentas e utensílios e demais recursos necessários à perfeita execução dos serviços elencados na tabela 1.1 deste TR, promovendo sua substituição quando necessário, para cumprir os níveis mínimos de serviços estabelecidos neste TR.

5.7.2. Para os serviços prestados fora do ambiente da CONTRATANTE, todos os recursos necessários à adequada prestação do serviço, tais como deslocamento, conexão de Internet, hardware e software, serão de responsabilidade da CONTRATADA.

5.8. Informações relevantes para o dimensionamento da proposta

5.8.1. A demanda do órgão tem como base as seguintes características:
5.8.1.1. Cada serviço do Grupo deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global.
5.8.1.2. O licenciamento das soluções de SIEM e de gerenciamento de vulnerabilidades deverá ser obrigatoriamente de propriedade da CONTRATADA e não poderá ser do tipo open source (software livre).
5.8.1.3. Devem englobar a alocação de equipamentos (quando exigido) hardware e/ou softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.
5.8.1.4. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante.
5.8.1.5. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

5.8.2. Junto à proposta comercial a licitante vencedora deverá apresentar:

5.8.2.1. Declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio da competitividade, conforme o disposto no item 1.7, do Anexo I, da IN SGD/ME nº 94, de 2022.

5.9. Especificação da garantia do serviço

5.9.1. Conforme item 4.11 - Requisitos de Garantia e Manutenção.

5.10. Procedimentos de transição e finalização do contrato

5.10.1. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:
5.10.1.1. Transição contratual, entendida como o processo de transferência dos conhecimentos e competências necessárias para prover a continuidade dos serviços contratados ou executados, portanto, a Contratada deverá realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da CONTRATANTE ou da nova empresa que continuará a execução dos serviços.
5.10.1.2. A transição contratual inicial é prevista para os itens 9 (segurança de redes) e (segurança de aplicação) do Grupo 1, não sendo prevista para os demais itens por se tratar de novos serviços a serem contratados pela ANAC.
5.10.1.3. A CONTRATADA deverá responsabilizar-se pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de informações, conhecimentos e procedimentos, no final dos contratos, aconteçam de forma precisa e responsável.
5.10.1.4. Será considerado como período de transição inicial, os 90 (noventa) dias corridos contados a partir do início da execução dos serviços. Neste período a CONTRATADA atuará conjuntamente com a equipe da ANAC priorizando a documentação e absorção de conhecimento para a continuidade dos serviços de TI e a mitigação de impacto nas atividades dos usuários.
5.10.1.5. No período de transição inicial, as metas de Níveis Mínimos de Serviço serão implementadas gradualmente, sendo consideradas as seguintes metas:
5.10.1.5.1. Para o 1º mês de execução contratual: 70% de cada uma das metas.
5.10.1.5.2. Para o 2º mês de execução contratual: 80% de cada uma das metas.
5.10.1.5.3. Para o 3º mês de execução contratual: 90% de cada uma das metas.
5.10.1.5.4. A partir do 4º mês de execução contratual: 100% de cada uma das metas.
5.10.1.6. Não ocorrerá período de transição caso não ocorra a substituição da empresa prestadora de serviços.
5.10.1.7. A simples aplicação de redutor por descumprimento dos indicadores Níveis Mínimos de Serviços (NMS) não exime a Contratada de outras sanções estabelecidas neste Termo de Referência.
5.10.1.8. Ao final do contrato de prestação dos serviços, a empresa CONTRATADA deverá fornecer, pelo período de 90 (noventa) dias corridos, todas as informações necessárias à transição para a nova CONTRATADA, além de elaborar e atualizar

toda a documentação que porventura não tenha sido devidamente gerada ou atualizada durante o período de vigência do contrato.
5.10.1.9. Ao término do contrato, seja por decurso de vigência ou por suspensão/cancelamento, promover:
5.10.1.9.1. A transição contratual efetuando a transferência de conhecimento para a equipe técnica da CONTRATANTE ou da nova pessoa jurídica, de todos os novos serviços implantados ou modificados, mediante documentação técnica em repositório adotado pela CONTRATANTE para esse fim.
5.10.1.9.2. Manter no mínimo por 90 (noventa) dias após o término do contrato os softwares utilizados para execução dos serviços objeto deste documento.
5.10.1.9.3. Disponibilizar as bases de dados dos softwares utilizados para execução dos serviços objeto deste documento.
5.10.1.10. Ao final do contrato de prestação dos serviços, a empresa CONTRATADA deverá exportar e permitir a conversão dos dados da ANAC dos sistemas de propriedade da CONTRATADA que contenham informações de workflow, comportamento dos usuários, regras de automação etc.
5.10.1.10.1. Pode ocorrer pela transferência de conhecimento, tecnologia e técnicas:
5.10.1.10.2. A manutenção dos recursos materiais e humanos necessários à continuidade do negócio por parte da Administração.
5.10.1.10.3. A entrega de versões finais dos produtos e da documentação.
5.10.1.10.4. A transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação.
5.10.1.10.5. A devolução de recursos.
5.10.1.10.6. A revogação de perfis de acesso.
5.10.1.10.7. A eliminação de caixas postais. e
5.10.1.10.8. Outras que se apliquem.

5.11. Mecanismos formais de comunicação

5.11.1. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

5.11.1.1. Ordem de Serviço;

5.11.1.2. Ata de Reunião;

5.11.1.3. Ofício;

5.11.1.4. Sistema de abertura de chamados;

5.11.1.5. E-mails e Cartas;

5.12. Formas de Pagamento
5.12.1. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

5.13. Manutenção de Sigilo e Normas de Segurança
5.13.1. O Contratado 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.
5.13.2. 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 do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos Anexo IV - Termo de Compromisso de Manutencao do Sigilo e Anexo V - Termo de Ciência.

6. Modelo de gestão do contrato

6. MODELO DE GESTÃO DO CONTRATO

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
6.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal

formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Preposto
6.5.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.
6.5.2. A Contratada deverá manter preposto da empresa, disponível para acionamento durante o período, tendo em vista tratar de serviços que visam aprimorar e preservar a segurança das informações sob a custódia da Anac e que em caso de ataque ou indisponibilidade as providências devem ser adotadas prontamente.
6.5.3. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

6.6. Reunião Inicial
6.6.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.
6.6.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.
6.6.2.1. A pauta desta reunião observará, pelo menos:
6.6.2.1.1. Presença do representante legal da contratada, que apresentará o seu preposto;
6.6.2.1.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
6.6.2.1.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
6.6.2.1.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
6.6.2.1.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

6.7. Fiscalização
6.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

6.8. Fiscalização Técnica
6.8.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI).
6.8.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II).
6.8.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III).
6.8.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).
6.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).
6.8.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

6.9. Fiscalização Administrativa
6.9.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).
6.9.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua

competência; (Decreto nº 11.246, de 2022, art. 23, IV).
6.9.3. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:
6.9.3.1. Verificação de aderência aos termos contratuais;
6.9.3.2. Apoiar o Gestor do contrato quanto às questões administrativas contratuais;
6.9.3.3. Apoiar o Fiscal Requisitante do Contrato na verificação da manutenção da necessidade, economicidade e oportunidade da contratação;
6.9.3.4. Apoiar ao Gestor do Contrato na manutenção do Histórico de Gestão do Contrato.

6.10. Gestor do Contrato
6.10.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).
6.10.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).
6.10.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).
6.10.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).
6.10.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6.10.6. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6.10.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. Critérios de medição e pagamento

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR) disposto neste item.
7.2. De maneira a uniformizar o entendimento quanto a classificação para incidentes e requisições de serviço de segurança da Informação, definem-se os níveis de criticidade como:

Tabela 7.1

NÍVEL DE CRITICIDADE	IMPACTO/DESCRIÇÃO
EMERGENCIAL	• Algum tipo de ataque que gerou indisponibilidade em servidores e sistemas críticos, afetando um ou mais usuários; • Infecção ou paralisação generalizada devido a ransomware ou algum outro tipo de malware;

	• Roubo ou vazamento de dados devido a falha humana ou técnica; • Algum tipo de impacto ou risco grave ao órgão ou a equipe de Segurança da Informação; • Quando o problema\incidente é denido com o nível de criticidade “EMERGENCIAL”.
ALTA	• Servidor de produção ou sistema crítico está apresentando instabilidade, degradação ou sofrendo ataques recorrentes que podem acarretar uma exploração ou vazamento de dados; • Alarmes de nível ALTA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; • Ocorrências\Incidentes\requisições relacionados a usuários definidos como VIP pelo CONTRATANTE; • Quando o problema\incidente é definido com o nível de criticidade "ALTA".
MÉDIA	• Nenhum serviço crítico está envolvido e não existe risco de perda de dados; • Alarmes de nível MÉDIO identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e necessitam de uma análise para validação; • Quando o problema\incidente é definido com o nível de criticidade "MÉDIA".
BAIXA	• Dúvidas ou apoio à implementação; • Mudanças planejadas; • Novas implementações; • Sugestões de novos recursos ou aprimoramento do Software; • Alarmes de nível BAIXA identificados por ferramentas de SIEM ou ferramenta de segurança que podem ser um falso positivo e • necessitam de uma análise para validação; • Evidências de um bloqueio ou tratativa automatizada; e • Quando o problema\incidente é definido com o nível de criticidade "BAIXA".

7.3. Para efeito desta contratação, estabelecem-se os seguintes níveis mínimos de serviços para a resposta e solução das requisições de serviço e incidentes. Os serviços serão medidos com base em indicadores e níveis mínimos de serviços, vinculados

a fórmulas de cálculo específicas, e deverão ser executados pela CONTRATADA e apurados mensalmente, de modo a alcançar as respectivas metas exigidas, conforme tabela a seguir.

7.4. A CONTRATADA deverá manter os seguintes níveis de qualidade para a prestação dos Serviços Gerenciados de Segurança:

7.4.1. Observação: 1% a cada 15 pontos, limitada a 30% do valor mensal previsto (soma dos itens).

7.4.1.1. Caso o desconto na fatura mensal ultrapasse o limite mensal preestabelecido, poderá ser aplicado na fatura do mês subsequente, à exceção do último mês de vigência do contrato.

Tabela 7.2

NÍVEIS MÍNIMOS DOS SERVIÇOS EXIGIDOS PARA O GRUPO 01				
Item	**Indicadores de Níveis de Serviço**	**Fórmula de Cálculo com base no mês calendário**	**Meta Exigida**	**Glosa por inadimplemento**
1	Índice de disponibilidade dos serviços de segurança da ANAC.	Total de tempo com disponibilidade no mês / total de tempo no mês X 100	>= 99,7 %	30 pontos (+5 pontos a cada 0,1% abaixo da meta)
2	Tempo máximo para correção de incidente nos serviços de segurança da ANAC, em caso de indisponibilidade.	Tempo = Hora do restabelecimento - Hora do início da indisponibilidade	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
3	Tempo máximo para correção de incidente nos serviços de segurança da ANAC, em caso de degradação de desempenho.	Tempo = Hora do restabelecimento - Hora do início da degradação de desempenho	<= 90 minutos	15 pontos (+5 pontos a cada 10 minutos excedentes)
4	Tempo máximo para triagem de incidentes de segurança	Tempo = Hora da triagem - Hora de entrada do evento de segurança	<= 15 minutos	5 pontos (+1 ponto a cada 5 minutos excedentes)
5	Tempo máximo para resposta de incidentes de segurança de gravidade emergencial	Tempo = Hora do início da resposta - hora da triagem	<= 30 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
6				

	Tempo máximo para resposta de incidentes de segurança de gravidade alta	Tempo = Hora do início da resposta - hora da triagem	<= 60 minutos	5 pontos (+3 pontos a cada 5 minutos excedentes)
7	Tempo máximo para resposta de incidentes de segurança de gravidade média e baixa	Tempo = Hora do início da resposta - hora da triagem	<= 240 minutos	3 pontos (+3 pontos a cada 5 minutos excedentes)
8	Tempo máximo para submissão de requisição de mudança para aplicação de patches e hotfixes de segurança para tratamento de vulnerabilidade ou ameaça emergente definidas como EMERGENCIAL\CRITICA e\ou ALTA	Tempo = Hora de conclusão do planejamento da requisição de mudança - hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente	<= 72 horas	5 pontos (+2 pontos a cada hora excedente)
9	Tempo máximo para resolução de requisições de serviços relacionadas aos produtos de UTM ou WAF.	Tempo = Hora da resolução da solicitação — hora de início da solicitação	<= 240 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
10	Tempo máximo para resolução das demais requisições de serviços	Tempo = Hora da resolução da solicitação — hora da solicitação	<= 24 horas	10 pontos (+3 pontos a cada hora excedente)
11	Tempo máximo para comunicação de incidentes definidos como EMERGENCIAL e ALTA aos gestores de TI da ANAC.	Tempo = Hora da comunicação — hora da triagem	<= 15 minutos	5 pontos (+2 pontos a cada 5 minutos excedentes)
12	Índice de cumprimento dos prazos acordados para a execução das Ordens de Serviço Exclusivas.	Prazo Real — (Prazo Acordado + 25%)	<= 0	15 pontos
13			<= 60 minutos	5 pontos (+2 pontos a

	Tempo máximo para abertura de chamados de suporte com terceiros (fabricantes e parceiros)	Tempo = Hora de abertura do chamado — hora da triagem		cada 5 minutos excedente)
14	Emissão de relatório mensal de atendimento de requisições e de incidentes	Tempo = Até 3º dia útil do mês seguinte	<= 72 horas	5 pontos (+2 pontos a cada 24 horas excedente)

7.5. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso a Contratada:
7.5.1. não produzir os resultados acordados,
7.5.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
7.5.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.
7.5.4. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços
7.6. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:
7.6.1. Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA:

Tabela 7.3

Item	Descrição	Referência	Glosa por inadimplemento
1	Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Por ocorrência	10 pontos
2	Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Por ocorrência	5 pontos
3	Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Por ocorrência	5 pontos
4	Finalizar um problema sem documentar a investigação	Por ocorrência	5 pontos

	realizada, a causa-raiz ou a solução aplicada.		
5	Fraudar, manipular ou descaracterizar indicadores /metas de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Por ocorrência	30 pontos
6	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Por profissional e por dia	30 pontos
7	Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	30 pontos
8	Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares) ou utilizar equipamento particular;	Por ocorrência	30 pontos
9	Realizar mudanças de configuração nas soluções de segurança sem autorização da unidade responsável.	Por regra incluída, alterada ou excluída.	15 pontos

7.6.2. Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA deixar de:

Tabela 7.4

Item	Descrição	Referência	Glosa por inadimplemento
1		Por ocorrência	10 pontos

	Cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.		
2	Cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança.	Por ocorrência	10 pontos
3	Executar testes de continuidade de cada solução de segurança da informação em alta disponibilidade a, no mínimo, cada 6 (seis) meses.	Por ocorrência	10 pontos
4	Atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança.	Por ocorrência	10 pontos
5	Apresentar mensalmente plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos.	Por ocorrência	20 pontos
6	Apresentar os relatórios consolidados conforme exigências do Termo de Referência até o dia 5° dia útil do mês subsequente.	Por dia de atraso	05 pontos
7	Apresentar relatórios, levantamentos ou inventários conforme demanda em até 3 dias úteis.	Por ocorrência	05 pontos
8	Manter o Configuration Management Database (CMDB) atualizado.	Por ocorrência	10 pontos
9	Manter a documentação e os desenhos das topologias atualizados e completos.	Por ocorrência	05 pontos
10			

	Notificar sobre ocorrências recorrentes.	Por ocorrência	05 pontos
11	Cumprir ou implementar as rotinas em conformidade com os processos de trabalho da Secretaria de Tecnologia e Transformação Digital	Por ocorrência	10 pontos
12	Elaborar auditorias de dados, consultas às bases de logs de transações ou relatórios diversos.	Por ocorrência	15 pontos
13	Analisar a viabilidade e o impacto da instalação de novas soluções ou correções.	Por ocorrência	05 pontos
14	Apresentar mensalmente proposta de melhorias no ambiente.	Por ocorrência	05 pontos
15	Cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pela ANAC.	Por ocorrência	15 pontos

7.6.3. Serão aplicadas glosas no caso de a CONTRATADA deixar de:

Tabela 7.5

Item	Descrição	Referência	Glosa por inadimplemento
1	Assegurar a disponibilidade dos canais de comunicação para estabelecimento da VPN.	Por ocorrência	20 pontos
2	Cumprir outras obrigações do TERMO DE COMPROMISSO	Por ocorrência	15 pontos
3	Ter preposto	Por ocorrência	20 pontos
4	Apresentar nota fiscal de faturamento com valor correto apurado pelo CONTRATANTE após aplicação das glosas	Por ocorrência	15 pontos
5			

	Cumprir prazo definido em ata de reunião	Por ocorrência	20 pontos
6	Atender o prazo definido no item 1.4.5 do "Anexo I - Especificações Técnicas" para o Gerente de Crise.	Por ocorrência	15 pontos

7.6.4. Serão aplicadas glosas à CONTRATADA no caso de:

Tabela 7.6

Item	Descrição	Referência	Glosa por inadimplemento
1	Não atingir nível mínimo de serviços, apurados em um período de 12 meses	3 meses consecutivos	10%
2	Não atingir nível mínimo de serviços, apurados em um período de 12 meses	5 meses alternados	10%
3	Não atingir nível mínimo de serviços, apurados em um período de 12 meses	6 meses consecutivos	20%
4	Inexecução parcial dos serviços mensais	50 a 69,9%	10%
5	Inexecução total dos serviços mensais	0 a 49,9%	20%

7.6.5. As retenções ou glosas no pagamento serão aplicadas quando a CONTRATADA:
7.6.6. Não atingir os valores mínimos aceitáveis fixados nos Critérios de Aceitação, não produzir os resultados ou deixar de executar as atividades contratadas;
7.6.7. Deixar de utilizar materiais e recursos humanos necessários e suficientes para fornecimento da Solução de Tecnologia da Informação, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.6.8. No cálculo de indicadores relacionados à disponibilidade, a apuração dos resultados desconsiderará períodos de indisponibilidades justificados, tais como:

a) Períodos de interrupção previamente acordados com o contratante;
b) Interrupção de serviços públicos essenciais à plena execução dos serviços (exemplo: suprimento de energia elétrica);
c) Indisponibilidade de acesso ao ambiente e/ou aos sistemas da rede, motivada por razões incontroláveis ou de força maior (exemplo: desastres naturais, enchentes, terremotos ou calamidade pública);
d) Falhas da infraestrutura que não aquela sob a responsabilidade do contratado;
e) Falhas em serviços ou ativos de TIC que tenham sido causadas pela ação de servidores ou colaboradores do contratante não relacionados ao contratado;
f) Outras eventualidades ocorridas durante a execução contratual mediante justificativa devidamente fundamentada do contratado.

7.7. Do recebimento

7.7.1. Os serviços serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo (Art. 140, I, a , da Lei nº 14.133 e Arts 22, X e 23, VII do Decreto nº 11.246, de 2022)

7.7.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.
7.7.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico (Art. 22, X, Decreto nº 11.246, de 2022).
7.7.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo (Art. 23, VII, Decreto nº 11.246, de 2022)
7.7.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.
7.7.6. 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.
7.7.7. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;
7.7.8. O Contratado fica obrigado 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.
7.7.9. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório (Art. 119 c/c art 140 da Lei nº 14133, de 2021)
7.7.10. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis
7.7.11. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades
7.7.12. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado 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 do contrato para recebimento definitivo.
7.7.13. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:
7.7.14. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (Art. 21, VIII, Decreto nº 11.246, de 2022).
7.7.15. 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;
7.7.16. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
7.7.17. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
7.7.18. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.
7.7.19. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
7.7.20. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.
7.7.21. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.8. Liquidação

7.8.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.
7.8.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.
7.8.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:
7.8.3.1. o prazo de validade;
7.8.3.2. a data da emissão;
7.8.3.3. os dados do contrato e do órgão CONTRATANTE;

7.8.3.4. o período respectivo de execução do contrato;
7.8.3.5. o valor a pagar; e
7.8.3.6. eventual destaque do valor de retenções tributárias cabíveis.
7.8.4. Havendo erro na apresentação da Nota Fiscal ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;
7.8.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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. 68 da Lei nº 14.133, de 2021.
7.8.6. A Administração deverá realizar consulta ao SICAF para:
a) verificar a manutenção das condições de habilitação exigidas no edital;
b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).
7.8.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, 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 CONTRATANTE.
7.8.8. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, 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.
7.8.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.
7.8.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

7.9. Prazo de pagamento
7.9.1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.
7.9.2. No caso de atraso pela CONTRATANTE, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de Custo da Tecnologia da Informação (ICTI) de correção monetária.

7.10. Forma de pagamento
7.10.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
7.10.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
7.10.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
7.10.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
7.10.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

7.11. Antecipação de pagamento
7.11.1. A presente contratação não permite a antecipação de pagamento.

7.12. Cessão de crédito Nota(s)
7.12.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020, conforme as regras deste presente tópico.
7.12.2. As cessões de crédito não fiduciárias dependerão de prévia aprovação da CONTRATANTE
7.12.3. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.12.4. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

7.12.5. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020).
7.12.6. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

8. Critérios de seleção do fornecedor

8. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

8.1. Forma de seleção e critério de julgamento da proposta
8.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO do Grupo.

8.1.2. Conforme indicado no item 4.24.2., o Anexo IX contém o modelo de apresentação da proposta comercial e a planilha de custos e formação de preços que deve ser entregue pelas empresas licitantes durante a fase de seleção do fornecedor.

8.1.3. Justificativa para impedimento das empresas contratadas para prestação do serviço de service desk e do serviço de sustentação de infraestrutura de TI (NOC):
8.1.3.1. O principal objetivo das empresas responsáveis pela execução do serviço de Service Desk e do serviço de sustentação de infraestrutura da Anac (NOC) é manter o pleno funcionamento dos recursos e serviços do ambiente de TIC e melhorar a qualidade dos serviços prestados aos seus usuários. Assim, sua prioridade é garantir a disponibilidade de acordo com os níveis estabelecidos.
8.1.3.2. Os serviços de SOC, de Service Desk e de NOC na Anac atuarão em tecnologias, processos e ambientes compartilhados, ao passo que suas atribuições serão distintas e complementares, uma vez que um SOC será responsável pela garantia da tríade de segurança: confidencialidade, integridade e disponibilidade. Por outro lado, as empresas responsáveis pelos serviços de Service Desk e pelos serviços de sustentação de infraestrutura de TI (NOC), concentrar-se-ão apenas na implementação de alguns dos controles de segurança no ambiente de infraestrutura, de estações de trabalho e de processos de trabalho.
8.1.3.3. Enquanto o objetivo das empresas prestadoras de NOC e de Service Desk é manter a disponibilidade e realizar configurações de segurança solicitadas, sejam elas em equipamentos de infraestrutura, estações de trabalho, ferramentas e processos de trabalho ou no atendimento aos usuários, o da empresa de serviços de SOC é encontrar lacunas e falhas segurança nos serviços prestados, softwares e hardwares configurados por aquelas empresas. Nessa perspectiva, a ISO 27001 considera a segregação de funções como um controle a ser aplicado para reduzir o risco.
8.1.3.4. Portanto, resta demonstrado o impedimento de as empresas contratadas para prestar o serviço de Service Desk e o serviço de sustentação de infraestrutura de TI (NOC) da Anac de participarem do certame licitatório oriundo do presente Termo de Referência.
8.2. Regime de execução
8.2.1. O regime de execução do contrato será por empreitada por preço unitário.
8.3. Exigências de habilitação
8.3.1. Habilitação jurídica
8.3.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.
8.3.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.
8.3.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br /empreendedor.
8.3.1.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores.
8.3.1.5. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores.
8.3.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

8.3.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.
8.3.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.
8.3.2. Habilitação fiscal, social e trabalhista
8.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.
8.3.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.
8.3.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS).
8.3.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.
8.3.2.5. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
8.3.2.6. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.
8.3.2.7. Caso o fornecedor seja considerado isento dos tributos Municipal/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
8.3.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.
8.3.3. Qualificação Econômico-Financeira
8.3.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples.
8.3.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art69, caput, inciso II).
8.3.3.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
8.3.3.4. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um).
8.3.3.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. e
8.3.3.6. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.
8.3.3.7. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.
8.3.3.8. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% do valor total estimado da contratação.
8.3.3.9. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei nº 14.133, de 2021, art65, §1º).
8.3.3.10. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

8.4. Qualificação Técnica

8.4.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.
8.4.2. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.
8.4.3. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

8.4.4. A licitante deverá apresentar planilha ponto a ponto que comprove o atendimento de todos os requisitos elencados no item 4 do Termo de Referência. Na planilha deverá indicar documento em que consta o cumprimento de cada um dos requisitos das especificações técnicas. As indicações devem ser assertivas, contendo página e parágrafo, link ou nome do documento referenciado para comprovação do item.
8.4.5. A LICITANTE deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas

Fiscais/Faturas, Notas de Empenho, endereço atual da CONTRATANTE e local em que foram prestados os serviços.
8.4.6. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
8.4.7. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
8.4.8. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.
8.4.9. Deverá ser entregue juntamente com os atestados a Planilha de Comprovação Técnica para o Grupo 1 – item 4 (Blue Team) e Grupo 3 – item 12 (Red Team), dada a necessidade de autonomia entre os serviços. Assim, caso a mesma licitante - ou sua subsidiária/controlada - oferte a melhor proposta para os itens 4 e 12, dada a ordem cronológica das etapas do processo de avaliação dos atestados, serão avaliados os atestados e cumprimento dos requisitos definidos para o Grupo 1. Se a licitante for tecnicamente habilitada para o Grupo 1, automaticamente será desclassificada para o Grupo 3, porém, se a licitante não for habilitada tecnicamente para o Grupo 1, serão avaliados os atestados e cumprimento dos requisitos definidos para o Grupo 3 e, em sendo o caso de cumprimento destes, será considerada tecnicamente habilitada para o Grupo 3.
8.4.10. Os serviços ofertados devem atender integralmente aos requisitos da especificação técnica, necessitando ser comprovados os requisitos da Planilha de Comprovação Técnica.

8.4.11. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

8.4.11.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.4.11.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.4.11.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

8.4.11.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

8.4.11.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

8.4.11.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.4.11.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.
8.4.12. Para os serviços do Grupo 1:
8.4.12.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, para a soluções especificadas a seguir, considerando as seguintes características mínimas:
8.4.12.2. Serviços de gestão de vulnerabilidade, por meio do fornecimento, instalação, prestação de serviços de suporte, administração e operação da solução para no mínimo, 750 (setecentos e cinquenta) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item 7 - Gestão de vulnerabilidades, exigidos no Grupo 1 deste certame.
8.4.12.3. Serviços de monitoramento e gestão de incidentes de segurança, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança através da análise de logs e pacotes, em redes com, no mínimo, 1500 (mil e quinhentos) Eventos por Segundo ou 75 GB/dia. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado no Item 5 - Monitoramento e correlação de
eventos de segurança da informação, exigidos no Grupo 1 deste certame.
8.4.12.4. Serviços estratégicos de governança, risco e conformidade de cibersegurança ou segurança da informação, prestados para instituição com no mínimo 1000 (mil) usuários de tecnologia e contemplando no mínimo elaboração de diagnósticos e avaliações de análise de gap (situação e lacunas), maturidade e conformidade (com leis, normas e melhores práticas), elaboração ou revisão de políticas, planos, procedimentos, indicadores e métricas de cibersegurança e/ou segurança da informação, especificado no item 1 - Apoio à Gestão de Segurança e 2 - Gestão de Ativos e Configuração Segura, exigidos no Grupo 1 deste certame.
8.4.13. Para os serviços referentes ao Grupo 2: Serviços de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI):
8.4.13.1. Experiência em projetos e operações de serviços de Inteligência de Ameaças Cibernéticas de, no mínimo, 20 (vinte) VIPs e 4 (quatro) quatro marcas em contrato de 12(doze) meses na realização de atividades de CTI.

8.4.14. Para os serviços referentes ao Grupo 3 - Testes de Invasão:
8.4.14.1. Atestado(s) ou Declarações de Capacidade Técnica, em nome da licitante, acompanhado do seu respectivo contrato, expedido(s) por pessoa jurídica de direito público ou privado, comprovando que:

a) executou os serviços de teste de invasão (PENTEST) em sistemas web, infraestrutura, API's ou aplicações mobile na quantidade mínima de 50 alvos para exploração de vulnerabilidades de segurança da informação em conformidade com boas práticas internacionais, em um contrato de 12 (doze) meses;

b) a Contratada deve apresentar um ou mais atestados de capacidade técnica que comprovem sua atuação na execução das atividades relacionadas à solução do Grupo 3, conforme descrito no Anexo III - Catálogo de Serviços, há pelo menos 2 (dois) anos.

8.5. Da Aplicação da Margem de Preferência

8.5.1. Não será aplicada margem de preferência na presente contratação.

9. Estimativas do Valor da Contratação

Valor (R$): 9.184.874,58

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de R$ 9.184.874,58 (nove milhões cento e oitenta e quatro mil oitocentos e setenta e quatro reais e cinquenta e oito centavos), conforme custos unitários apostos na tabela 1.1.

10. Adequação orçamentária

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.1.1. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: 20214/113214;

II) Fonte de Recursos: 1050;

III) Programa de Trabalho: 26125310429120001 / 229038;

IV) Elemento de Despesa: 339040;

V) Plano Interno: 20TSEC250XX;

10.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. Papéis e Responsabilidades

11.1. São obrigações da CONTRATANTE:

11.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

11.1.2. 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;

11.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

11.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

11.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

11.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

11.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

11.1.8. 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.

11.2. São obrigações do CONTRATADO:

11.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

11.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

11.2.3. 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;

11.2.4. 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;

11.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

11.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

11.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

11.2.8. 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, os modelos de dados e as bases de dados à Administração;

11.2.9. fazer a transição contratual, quando for o caso.

11.2.10. manter, durante a execução dos serviços, vínculo celetista com todos os profissionais alocados para execução dessas ordens de serviço, não sendo permitida a subcontratação parcial ou total do objeto, com exceção do previsto no item 4.21.

12. Responsáveis

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

Despacho: Portaria nº 15003, DE 10 de julho de 2024

FELIPE SANTOS SARMANHO

Integrante Requisitante

Assinou eletronicamente em 14/04/2025 às 13:26:37.

Despacho: Portaria nº 15003, DE 10 de julho de 2024

REGINALDO LIRA DE ARAUJO

Integrante Técnico

Assinou eletronicamente em 14/04/2025 às 12:09:29.

Despacho: Portaria nº 15003, DE 10 de julho de 2024

FABIANO BENEDITO DE SIQUEIRA BENTO

Integrante Administrativo

Assinou eletronicamente em 14/04/2025 às 12:15:09.

FERNANDO ANDRE COELHO MITKIEWICZ

Autoridade competente

Assinou eletronicamente em 15/04/2025 às 09:36:42.

Anexo ao Termo de Referência

Especificações Técnicas

1. ESPECIFICAÇÃO DOS SERVIÇOS GERENCIADOS DE SEGURANÇA LOTE 01

1.1. **APOIO À GESTÃO DE SEGURANÇA**

1.1.1. A contratada deverá fornecer o serviço de gerenciamento para apoio a GRC (Governança, Risco e Compliance).

1.2. A composição do serviço fornecido pela CONTRATADA deverá cobrir obrigatoriamente os seguintes grupos:

1.1.1.1. Gestão de Riscos de TI: para apoiar e executar os processos de gestão de riscos de TI da CONTRATANTE.

1.1.1.2. Gestão de Continuidade: para apoiar na elaboração e manutenção dos planos de continuidade e de recuperação dos serviços e soluções de TI da CONTRATANTE.

1.1.1.3. Gestão de Políticas de Segurança da Informação: para apoiar, revisar, controlar e manter as políticas, normas e procedimentos de segurança da informação já estabelecidas no ambiente da CONTRATANTE e as demais que vierem a ser estabelecidas.

1.1.1.4. Gestão de Conformidade: para validar, acompanhar e avaliar se as políticas de segurança estabelecidas pela CONTRATANTE estão sendo respeitadas no âmbito da ANAC.

1.1.2. Anualmente a CONTRATADA deverá elaborar e revisar até 15 políticas e normas de segurança da informação baseados no padrão internacional da ISO 27001:2022 e nas normativos nacionais, que deverão ser indicadas pela CONTRATANTE, ou aprovadas em caso de indicação da CONTRATADA.

1.1.2.1. A contratada deverá elaborar e revisar procedimentos operacionais afetos aos serviços e ativos sob responsabilidade da contratada, sem limitação de quantidade, tantos quantos forem necessários.

1.1.2.2. Os procedimentos operacionais afetos aos serviços e ativos sob responsabilidade de outras contratadas serão de responsabilidade de elaboração destas.

1.1.3. É requisito a revisão, criação e implementação dos seguintes planos, procedimentos e políticas:

1.1.3.1. Política de Segurança da Informação.

1.1.3.2. Manual de gestão de Segurança da Informação.

1.1.3.3. Plano de gestão de vulnerabilidades.

1.1.3.4. Plano de resposta a incidentes.

1.1.3.5. Procedimentos de Gestão de Risco e Governança em Segurança da Informação.

1.1.4. Todos as políticas, manuais, planos e procedimentos estabelecidos pela contratada devem seguir as recomendações das normas técnicas ISO/IEC 27001, ISO/IEC 27002, NBR ISO/IEC 17799, ISO/TR 13335, Lei 12.965 (Marco Civil da Internet), lei 13.709 (LGPD), CIS e MITRE ATT&CK, seguindo também e melhores práticas de mercado e normativos direcionados à Administração Pública Federal.

1.1.5. Processos

1.1.5.1. A CONTRATADA deverá realizar de forma semestral uma avaliação prévia no ambiente computacional da CONTRATANTE, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado pela CONTRATANTE

1.1.5.2. O passo que segue será a definição e adoção de linha de base para avaliação do ambiente. A avaliação de conformidade do ambiente da CONTRATANTE, deverá ser feita pela CONTRATADA tomando como linha de base as políticas e normas de segurança da CONTRATANTE, não se detendo apenas a esta, mas também adicionando a esta análise linhas de base de fabricantes e frameworks de segurança, que tenha relação com o ambiente tecnológico da CONTRATANTE e seu negócio fim, incluindo leis, normativos, políticas e padrões

1.1.5.3. Após definição de linha de base, a CONTRATADA deverá submeter tal linha de base para aprovação da CONTRATANTE, antes de iniciar o

processo de varredura do ambiente. Caberá única e exclusivamente ao time de segurança da informação da CONTRATANTE a aprovação de tal linha de base

1.1.5.4. Alcançada a aprovação da linha de base, será de responsabilidade da CONTRATADA a varredura de todo os recursos do ambiente da CONTRATANTE, comparando os itens de controle da linha de base estabelecida, utilizando para tal a solução descrita no presente termo de referência. Nem todos os itens de controle são identificados automaticamente por uma varredura da solução de conformidade, como por exemplo o uso de identificação (crachá) em área controlada, todavia tais itens não podem ser negligenciados para avaliação final, logo caberá a CONTRATADA definir métodos e processos para avaliação de tais controles.

1.1.5.5. Após o término das varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo do resultado alcançado, isso quer dizer, que devem ser informados à CONTRATANTE apenas resultados que conferem com a linha de base estabelecida

1.1.5.6. Após análise de falso positivo, a CONTRATADA deverá informar à CONTRATANTE as não conformidades encontradas.

1.1.5.7. A CONTRATANTE possui um processo de gestão de configuração e mudança, sobre sua governança, logo cabe única e exclusivamente à CONTRATANTE liberar ou autorizar toda e qualquer mudança, sugerida para correção de uma não conformidade. Sendo assim, nenhuma mudança deve ser realizada, sem que antes haja a liberação da mesma pela CONTRATANTE

1.1.5.8. Uma vez autorizada a mudança para correção de uma determinada não conformidade, caberá a CONTRATADA o acompanhamento das correções de não conformidade encontradas no ambiente, as quais serão realizadas pela equipe técnica da CONTRATANTE. A correção das não conformidades serão de responsabilidades da CONTRATANTE.

1.1.5.9. Para as não conformidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno, que para serem aplicadas ao ambiente, deverão obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores

1.1.5.10. A CONTRATADA deverá apoiar na definição de um processo de gestão de continuidade de serviços e soluções de TI. As atividades de gestão de continuidade a serem executadas pela CONTRATADA, incluem, mas não se limitam à:

1.1.5.10.1. Definição e mapeamento de processo de gestão de continuidade e recuperação de serviços e soluções de TI da CONTRATANTE.

1.1.5.10.2. Elaboração e manutenção dos planos de continuidade e de recuperação dos serviços e soluções de TI da CONTRATANTE.

1.1.5.11. Realizar Análise de Impacto no negócio (Business Impacto Analysis – BIA) da CONTRATANTE, com objetivo de:

1.1.5.11.1. Avaliar a criticidade dos processos tecnológicos de sistemas de informação.

1.1.5.11.2. Estimar a importância dos ativos de sustentação tecnológica da organização.

1.1.5.11.3. Definir em conjunto com a CONTRATANTE os tempos máximos de parada e recuperação (RTO – Recovery Time Objective) e de perda de dados (RPO – Recovery Point Objective).

1.1.5.11.4. Criar e acompanhar Testes e Exercícios, que permitam a avaliação da efetividade dos Planos de Continuidade e de Recuperação.

1.1.5.11.5. Elaborar relatórios de testes realizados.

1.1.5.12. Todos os procedimentos e processos solicitados neste texto devem ser entregue em fase de projeto, e após aceite da CONTRATANTE, deve ser designado um profissional da CONTRATADA que deve ser dedicado ao

projeto, para acompanhamento da evolução das indicações realizadas, monitoramento do processo, e revisão para melhorias.

1.1.5.13. A CONTRATADA deverá apoiar as atividades de análise auditorias de segurança internas: avaliação sistemática das políticas, normas, procedimentos e controles de segurança existentes, por meio de revisões de controles, lacunas e elaboração relatórios detalhados com recomendações para melhoria e planos de ação conetiva.

1.1.5.14. A CONTRATADA deverá apoiar as atividades de análise de auditorias de segurança externas: avaliar a postura de segurança da ANAC, definindo escopo, gerenciando o processo de auditoria, revisando relatórios, implementando recomendações e acompanhando o progresso das ações corretivas, visando garantir a conformidade, identificar vulnerabilidades e fortalecer as medidas de segurança.

1.1.5.15. Os profissionais habilitados para a torre de apoio à Gestão de Segurança deverão ser dedicados de segunda à sexta-feira das 08:00 às 18:00, na modalidade remota, sendo necessário o comparecimento presencial sempre que solicitado pela CONTRATANTE. O comparecimento será solicitado com pelo menos 48h de antecedência.

1.1.5.16. Os resultados dos assessments e planos podem servir de insumo para alteração nos SLAs e entregáveis, que devem ser combinados entre CONTRATADA e CONTRATANTE.

1.1.6. Ferramentas

1.1.6.1. Para a execução dos serviços de apoio à gestão de segurança, a CONTRATADA poderá utilizar as soluções e ferramentas já em uso pela ANAC. Caso identifique a necessidade de ferramentas adicionais, as mesmas poderão ser fornecidas pela CONTRATADA, sem custos adicionais à CONTRATANTE, sendo permitido o uso de soluções open source. A relação de ferramentas em uso pela Anac está listada no Anexo II - Ambiente Tecnológico.

1.1.6.1.1. No caso de adoção de ferramentas open source, a instalação deverá ser feita em ambiente computacional disponibilizado pela CONTRATANTE, podendo ser on-premise ou em cloud, e ao final do contrato, a ferramenta instalada será mantida no ambiente da ANAC, inclusive com seus dados.

1.1.6.1.2. No caso de adoção de ferramentas comerciais que não sejam de propriedade da ANAC, a instalação poderá ser feita no ambiente computacional da ANAC ou da CONTRATADA, e ao final do contrato, os dados brutos deverão ser disponibilizados para a ANAC, em formato XML, JSON, CSV, ou outro que venha a ser aceito pela CONTRATANTE.

1.1.7. Os profissionais habilitados para o serviço devem possuir as seguintes características:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação OU de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo de 12 (doze) meses em acompanhamento, auditoria e controles de conformidade e risco de TI

	Não existe restrição ou limite para acúmulo de certificações em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos na equipe técnica de GRC
Treinamentos/ Certificações	1. Certificação PMI-PMP Project Management Professional (obrigatório) Uma das seguintes certificações: 2. Certificação ISFS - Information Security Foundation based on ISO/IEC 27001 ou 3. CISSP - Certified Information Systems Security Professional ou equivalente ou 4. ISO/IEC 27005 Senior Lead Risk Manager ou equivalente ou 5. CISM (Certified Information Security Manager) ou equivalente.

1.1.7.1. É preciso ter pelo menos uma das certificações da tabela acima, ou equivalente.

1.1.7.1.1. A equipe deve ser dimensionada para execução dos serviços durante a vigência da ordem de serviço, cabendo a contratada gerenciar eventuais ausências, como férias, licenças para tratamento de saúde, entre outras situações.

1.1.7.2. Entregas a Serem Realizadas

1.1.7.2.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de Políticas de segurança criadas	Soma de políticas e normas de segurança criadas	Políticas de segurança criadas	Políticas de segurança criadas	Número total de Políticas de segurança criadas
Quantitativo de políticas de segurança revisadas	Soma de políticas e normas de segurança revisadas	Políticas de segurança revisadas	Políticas de segurança revisadas	Número total de Políticas de segurança revisadas
Quantitativo de políticas de segurança validadas	Soma de políticas e normas de segurança validadas	Políticas de segurança validadas	Políticas de segurança validadas	Número total de Políticas de segurança validada
Quantitativo de políticas de segurança avaliadas	Soma de políticas e normas de segurança avaliadas	Políticas de segurança avaliadas	Políticas de segurança avaliadas	Número total de Políticas de segurança avaliadas

1.2. GESTÃO DE ATIVOS E CONFIGURAÇÃO SEGURA

1.2.1. A execução desse serviço tem como objetivo o atendimento dos controles e medidas de segurança presentes no framework do Programa de Privacidade e Segurança da Informação – PPSI/SGD:

1.2.1.1. **Controle 1 - inventário e controle de ativos corporativos:** A gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis. dispositivos de rede. dispositivos não computacionais. Internet das Coisas (IoT). e servidores) conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da ANAC. Inclui a identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

1.2.1.2. **Controle 2 - inventário e controle de ativos software:** A gestão ativa (inventariar, rastrear e corrigir) de todos os softwares (sistemas operacionais e aplicações) na rede para que apenas o software autorizado seja instalado e possa ser executado, e que o software não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.

1.2.1.3. **Controle 4 – configuração segura de ativos corporativos e software:** Estabelecer e manter a configuração segura de ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis. dispositivos de rede. dispositivos não computacionais/IoT. e servidores) e software (sistemas operacionais e aplicações).

1.2.2. Atividades a serem executadas pela CONTRATADA:

1.2.3. Inventário e controle de ativos corporativos

1.2.3.1. Manutenção do inventário de ativos da ANAC preciso, detalhado e atualizado, considerando os ativos corporativos com potencial para armazenar ou processar dados e considerando as melhores práticas da área quanto às informações a serem mantidas na base de dados. A revisão do inventário de todos os ativos corporativos deve ocorrer semestralmente. A atualização do inventário deverá ocorrer constantemente na medida em que houver a inserção, atualização ou retirada de ativos no parque computacional da ANAC.

1.2.3.2. Definição e execução de processos para endereçamento de ativos não autorizados, a serem executados semanalmente.

1.2.3.2.1. Para a detecção e identificação de ativos, poderão ser utilizadas ferramentas de descoberta ativa ou passiva, bem como a análise dos logs DHCP ou uso de ferramenta de gestão de endereçamento IP para atualização do inventário e endereçamento dos ativos não autorizados.

1.2.4. Inventário e controle de ativos de software

1.2.4.1. Estabelecimento e manutenção de um inventário detalhado de todos os softwares licenciados instalados em ativos corporativos, considerando as melhores práticas da área quanto às informações a serem mantidas na base de dados. A revisão e atualização do inventário de software deve ocorrer semestralmente.

1.2.4.2. Definição e execução de processos para assegurar que apenas software atualmente suportado seja designado como autorizado no inventário de software para ativos, documentando exceções para softwares não suportados, mas necessários ao cumprimento das missões da ANAC, detalhando controles de mitigação e aceitação do risco residual. A revisão do inventário de software deve ser realizada mensalmente.

1.2.4.3. Definição e execução de processos para endereçamento de softwares não autorizados, a serem executados semanalmente.

1.2.4.4. Definição e implantação de controles técnicos para garantir que apenas bibliotecas e scripts autorizados tenham permissão de ser carregados ou executados, impedindo ou bloqueando a execução ou carga dos elementos não autorizados.

1.2.5. Configuração segura de ativos corporativos e software

1.2.5.1. Estabelecimento e manutenção de um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis. dispositivos não computacionais/IoT. e servidores) e software (sistemas operacionais e aplicações). A documentação deve ser revisada e atualizada anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança.

1.2.5.2. Estabelecimento e manutenção de um processo de configuração segura para infraestrutura de rede. A documentação deve ser revisada e atualizada anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança.

1.2.5.3. Gestão de contas padrão nos ativos e softwares corporativos, a serem executados mensalmente.

1.2.5.4. Identificação e mapeamento de serviços desnecessários nos ativos e softwares corporativos, a serem executados mensalmente.

1.2.5.4.1. Nas definições das baselines de segurança, deverão ser observadas as definições da Política de Segurança da Informação da ANAC, bem como os demais requisitos estabelecidos para a Administração Pública Federal. Como referência, devem ser utilizados benchmarks de segurança, guias de segurança ou checklists publicamente desenvolvidos, verificados e suportados.

1.2.6.Ferramentas

1.2.6.1. Para a execução dos serviços de gestão de ativos e configuração segura, a CONTRATADA poderá utilizar as soluções e ferramentas já em uso pela ANAC. Caso identifique a necessidade de ferramentas adicionais, as mesmas poderão ser fornecidas pela CONTRATADA, sem custos adicionais à CONTRATANTE, sendo permitido o uso de soluções open source. A relação de ferramentas em uso pela Anac está listada no Anexo II - Ambiente Tecnológico.

1.2.6.1.1. No caso de adoção de ferramentas open source, a instalação deverá ser feita em ambiente computacional disponibilizado pela CONTRATANTE, podendo ser on-premise ou em cloud, e ao final do contrato, a ferramenta instalada será mantida no ambiente da ANAC, inclusive com seus dados.

1.2.6.1.2. No caso de adoção de ferramentas comerciais que não sejam de propriedade da ANAC, a instalação poderá ser feita no ambiente computacional da ANAC ou da CONTRATADA, e ao final do contrato, os dados brutos deverão ser disponibilizados para a ANAC, em formato XML, JSON, CSV, ou outro que venha a ser aceito pela CONTRATANTE.

1.2.7.A contratada deverá atuar no estabelecimento e execução de processos relacionados aos respectivos controles, bem como no apoio e orientação quanto às ações necessárias para o aumento da maturidade da ANAC junto a demais contratos, de acordo com as medidas de segurança de cada um dos controles.

1.2.8. A CONTRATADA deverá revisar as políticas e os processos relacionados aos temas já existentes na ANAC e, na sua ausência, deverá providenciá-los, em até 90 (noventa) dias do início da execução dos serviços. A CONTRATADA irá propor

um cronograma de entrega dos processos, revisados ou escritos, para acompanhamento da equipe de fiscalização do contrato.

1.2.9. Perfil profissional:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação OU de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Possuir no mínimo 03 anos de experiência na área de segurança da informação.
Treinamentos/ Certificações	Possuir ao menos 1 (uma) das certificações abaixo: • CompTIA Security+ ou equivalente. • CCNA Security+ ou equivalente. • CEH Certified Ethical Hacker ou OSCP Offensive Security Certified Professional. • Check Point Certified Security Administrator (CCSA) ou equivalente. • Certificação em administração de solução de em Endpoint ou EDR. • F5 BIG-IP Certified Administrator, F5 BIG-IP ASM Certified Technical Specialist ou F5 BIG-IP LTM Certified Technical Specialist. • Certificação em administração de solução DDoS. • Microsoft 365 Certified: Security Administrator Associate, Microsoft Certified. • Associate ou Microsoft Certified: Security, Compliance, and Identity Fundamentals. • EXIN Information Security Management Professional based on ISO/IEC 27001. • ISO 27001:2013 Auditor Interno. • ISO 27001:2022 Auditor Líder. • ISO 27001:2022 Lead Implementer.

1.2.10. Entregas a Serem Realizadas

1.2.10.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Inventário de ativos corporativos	Soma de ativos corporativos com todas as informações necessárias preenchidas.	Ativos corporativos	Ativos corporativos	Manutenção do inventário de ativos da ANAC preciso, detalhado e atualizado
Detecção de Ativos Não Autorizados	Número de ativos não autorizados detectados semanalmente.	Ativos corporativos	Ativos corporativos	Ativos não autorizados detectados pelas ferramentas de descoberta ativa/passiva ou análise de logs DHCP
Inventário de ativos de software	Soma de ativos de software inventariados com todas as informações necessárias preenchidas.	Ativos de software	Ativos de software	Manutenção do inventário de ativos da ANAC preciso, detalhado e atualizado
Detecção de Ativos de software Não Autorizados	Número de softwares não autorizados detectados semanalmente.	Ativos de software	Ativos de software	Ativos de software não autorizados detectados
Conformidade com Configurações Seguras	Percentual de ativos e softwares configurados de acordo com as diretrizes de segurança.	Configuração segura	Configuração segura	Percentual de ativos e softwares configurados de acordo com as diretrizes de segurança.
Gestão de contas padrão	Percentual de contas padrão que foram alteradas ou desativadas.	Contas padrão	Configuração segura	Percentual de Contas Padrão Gerenciadas
Identificação e mapeamento de serviços desnecessários	Percentual de serviços desnecessários identificados em relação ao total de serviços.	Serviços desnecessários	Configuração segura	Percentual de Serviços Desnecessários Identificados
Definições das baselines de segurança	Percentual de ativos e softwares que atendem às baselines de segurança definidas	Baselines de segurança	Configuração segura	Conformidade com Baselines de Segurança

1.3. GESTÃO DE CONTA, CONTROLE DE ACESSO E AUDITORIA

1.3.1. A execução desse serviço tem como objetivo o atendimento dos controles e medidas de segurança presentes no framework do Programa de Privacidade e Segurança da Informação – PPSI/SGD:

1.3.1.1. **Controle 5 - gestão de contas:** Definição e execução de processos para atribuir e gerenciar autorização de credenciais para contas de usuário, incluindo contas de administrador, bem como contas de serviço, de ativos corporativos e software.

1.3.1.2. **Controle 6 - gestão do controle de acesso:** Definição e execução de processos para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, administrador e serviço para ativos e softwares corporativos.

1.3.1.3. **Controle 8 – gestão de registros de auditoria:** A gestão ativa (coletar, alertar, analisar e reter) de logs de auditoria de eventos.

1.3.2. Atividades a serem executadas pela CONTRATADA:

1.3.3. **Gestão de contas**

1.3.3.1. Manutenção do inventário de todas as contas gerenciadas na ANAC, incluindo contas de usuário e administrador, considerando as melhores práticas da área quanto às informações a serem mantidas no inventário. A CONTRATADA deverá validar se todas as contas ativas estão autorizadas, em uma programação recorrente a ser executada mensalmente.

1.3.3.2. Estabelecimento e manutenção de inventário de contas de serviço, considerando as melhores práticas da área quanto às informações a serem registradas. A CONTRATADA deverá validar se todas as contas ativas estão autorizadas, em uma programação recorrente a ser executada mensalmente.

1.3.4. **Gestão do controle de acesso**

1.3.4.1. Estabelecimento e execução de processo para concessão de acesso aos ativos corporativos mediante nova contratação, concessão de direitos ou mudança de função de um usuário.

1.3.4.2. Estabelecimento e execução de processo para revogação de acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

1.3.4.3. Estabelecimento e manutenção de inventário dos sistemas de autenticação e autorização da ANAC, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto. O inventário deve ser revisado e atualizado semestralmente.

1.3.4.4. Definição e manutenção do controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da ANAC. A CONTRATADA deverá realizar análises de controle de acesso de ativos corporativos para validar se todos os privilégios estão autorizados, em uma programação recorrente anual.

1.3.5. **Gestão de registros de auditoria**

1.3.5.1. Manter o processo de gestão de log de auditoria da ANAC, revisando e atualizando a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.

1.3.5.2. Gestão da coleta de logs de auditoria, garantindo que o log tenha sido habilitado em todos os ativos.

1.3.5.3. Gestão dos repositórios de logs, monitorando as capacidades de processamento e armazenamento adequados para a guarda dos registros de auditoria.

1.3.5.4. Gestão da coleta de logs de auditoria detalhados, garantindo que o log de ativos corporativos contendo dados sensíveis contenham elementos e informações úteis em eventual investigação forense.

1.3.5.5. Realizar análises de logs de auditoria para detecção de anomalias ou eventos anormais que possam indicar uma ameaça potencial. A CONTRATADA deverá realizar as revisões semanalmente.

1.3.6.Ferramentas:

1.3.6.1. Para a execução dos serviços de gestão de conta, controle de acesso e auditoria, a CONTRATADA poderá utilizar as soluções e ferramentas já em uso pela ANAC. Caso identifique a necessidade de ferramentas adicionais, as mesmas poderão ser fornecidas pela CONTRATADA, sem custos adicionais à CONTRATANTE, sendo permitido o uso de soluções open source. A relação de ferramentas em uso pela Anac está listada no Anexo II - Ambiente Tecnológico.

1.3.6.1.1. No caso de adoção de ferramentas open source, a instalação deverá ser feita em ambiente computacional disponibilizado pela CONTRATANTE, podendo ser on-premise ou em cloud, e ao final do contrato, a ferramenta instalada será mantida no ambiente da ANAC, inclusive com seus dados.

1.3.6.1.2. No caso de adoção de ferramentas comerciais que não sejam de propriedade da ANAC, a instalação poderá ser feita no ambiente computacional da ANAC ou da CONTRATADA, e ao final do contrato, os dados brutos deverão ser disponibilizados para a ANAC, em formato XML, JSON, CSV, ou outro que venha a ser aceito pela CONTRATANTE.

1.3.7.A contratada deverá atuar no estabelecimento e execução de processos relacionados aos respectivos controles, bem como no apoio e orientação quanto às ações necessárias para o aumento da maturidade da ANAC junto a demais contratos, de acordo com as medidas de segurança de cada um dos controles.

1.3.8. A CONTRATADA deverá revisar as políticas e os processos relacionados aos temas já existentes na ANAC e, na sua ausência, deverá providenciá-los, em até 90 (noventa) dias do início da execução dos serviços. A CONTRATADA irá propor um cronograma de entrega dos processos, revisados ou escritos, para acompanhamento da equipe de fiscalização do contrato.

1.3.9. Perfil profissional:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação OU de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Possuir no mínimo 03 anos de experiência na área de segurança da informação.
Treinamentos/ Certificações	Possuir ao menos 1 (uma) das certificações abaixo: • CompTIA Security+ ou equivalente. • CCNA Security+ ou equivalente.

	• CEH Certified Ethical Hacker ou OSCP Offensive Security Certified Professional. • Check Point Certified Security Administrator (CCSA) ou equivalente. • Certificação em administração de solução de em Endpoint ou EDR. • F5 BIG-IP Certified Administrator, F5 BIG-IP ASM Certified Technical Specialist ou F5 BIG-IP LTM Certified Technical Specialist. • Certificação em administração de solução DDoS. • Microsoft 365 Certified: Security Administrator Associate, Microsoft Certified. • Associate ou Microsoft Certified: Security, Compliance, and Identity Fundamentals. • EXIN Information Security Management Professional based on ISO/IEC 27001. • ISO 27001:2013 Auditor Interno. • ISO 27001:2022 Auditor Líder. • ISO 27001:2022 Lead Implementer.

1.3.10. Entregas a Serem Realizadas

1.3.10.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Inventário de contas gerenciadas	Soma de contas gerenciadas	Inventário de contas gerenciadas	Gestão de contas	Manutenção do inventário de todas as contas gerenciadas na ANAC, incluindo contas de usuário e administrador
Contas ativas não autorizadas	Soma de contas ativas não autorizadas detectadas durante as validações.	Contas ativas não autorizadas	Gestão de contas	Número de contas ativas não autorizadas detectadas durante as validações.
Inventário de contas de serviço	Soma de contas de serviço	Inventário de contas de serviço	Gestão de contas	Manutenção do inventário de todas as contas de serviço.
Contas de serviço não autorizadas	Soma de contas de serviço não autorizadas	Contas de serviço não autorizadas	Gestão de contas	Número de contas de serviço não

	detectadas durante as validações.			autorizadas detectadas durante as validações.
Gestão do controle de acesso	Soma de acessos concedidos e revogados	Acessos concedidos e revogados	Gestão do controle de acesso	Descrição dos acessos concedidos e revogados
Inventário de sistemas de autenticação e autorização	Descrição dos sistemas de autenticação e autorização	Sistemas de autenticação e autorização	Gestão do controle de acesso	Manutenção de inventário dos sistemas de autenticação e autorização
Conformidade com Controle de Acesso Baseado em Funções	Percentual de acessos concedidos de acordo com as funções documentadas.	Controle de acesso baseado em funções	Gestão do controle de acesso	Percentual de acessos concedidos de acordo com as funções documentadas.
Cobertura de Coleta de Logs	Percentual de ativos com logs de auditoria habilitados.	Logs de Auditoria	Gestão de registros de auditoria	Gestão da coleta de logs de auditoria, garantindo que o log tenha sido habilitado em todos os ativos
Capacidade de Armazenamento dos Repositórios	Percentual de utilização da capacidade de armazenamento dos repositórios de logs.	Capacidade de Armazenamento	Gestão de registros de auditoria	Percentual de utilização da capacidade de armazenamento dos repositórios de logs.

1.4. GESTÃO DE INCIDENTES DE SEGURANÇA (Blue Team)

1.4.1. Este serviço tem por objetivo analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de SI. Tal serviço deverá ser executado obedecendo as normas ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27005 e o framework NIST de resposta a incidente de segurança da informação e boas práticas de mercado.

Serviços de Resposta a Incidentes de Segurança		
Grupo de Serviço	ID	Serviço
Resposta a incidentes de segurança	1	Identificação da causa
	2	Tratamento da causa
	3	Aplicação da correção
	4	Validação do contorno do incidente
	5	Encerramento do registro do incidente

1.4.2. Os profissionais estimados para prestar os serviços de gestão de incidentes de segurança (Blue Team) deverão gerenciar a ferramenta de SIEM do serviço de monitoramento e visibilidade de ataques cibernéticos.

1.4.3. O Serviço de Gestão de Incidentes de Segurança deverá ser prestado em período integral (24x7x365) para o tratamento de incidentes de segurança da informação em regime remoto. Em caso de ocorrência de grave incidente de segurança que implique em comprometimento de disponibilidade, integridade ou confidencialidade das informações da ANAC, o atendimento deverá ser presencial, nas dependências do CONTRATANTE (sede da ANAC).

1.4.4. Os casos de grave incidente de segurança devem ser liderados por um Gerente de Crise, que deve possuir certificação CISSP (Certified Information Systems Security Professional) ou comprovada experiência no tratamento de incidentes de segurança de grande impacto técnico e institucional.

1.4.5. O Gerente de Crise deverá estar presencialmente nas dependências do CONTRATANTE em até 12 (doze) horas após a abertura do incidente.

1.4.6. Durante os horários de prestação dos serviços de Gestão de Incidentes de Segurança não serão permitidas ações como "SLA HOLD" ou qualquer recurso similar que possa vir mascarar ou paralisar o real tempo de atendimento destas requisições.

1.4.7. O Serviço de Gestão de Incidentes de Segurança será responsável por monitorar e reagir a eventos e incidentes de SI em equipamentos, softwares e demais componentes do ambiente computacional do CONTRATANTE, envolvendo, mas não se limitando em: identificar, classificar, analisar e solucionar incidentes que possam comprometer os requisitos de segurança da informação definidos pela ANAC.

1.4.8. Os canais de comunicação para tratamento dos incidentes devem ser as ferramentas de suporte definidas pelo CONTRATANTE, tais quais, telefone, ferramenta ITSM e e-mail, não se limitando a estas.

1.4.9. O início do processo de resposta a incidente de segurança da informação se dará após etapa de Monitoramento e correlação de eventos de segurança da informação, que consiste na atividade de observação ou recebimento de evento até sua classificação, comunicação (quando aplicável) e encaminhamento para o grupo de resposta a incidente de segurança (CSIRT - Blue Team) e sua respectiva ABERTURA como incidente.

1.4.10. Poderá também o corpo técnico de segurança do CONTRATANTE a qualquer tempo abrir um incidente de segurança da informação. A CONTRATADA deverá monitorar o padrão de acessos ao ambiente e definir, com o aval do CONTRATANTE, os limites (thresholds) a partir do qual caracterizarão incidente de Segurança da Informação.

1.4.11. Após o incidente de segurança ser ABERTO, será de responsabilidade do grupo de resposta a incidente de segurança (CSIRT — Blue Team) da CONTRATADA analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

1.4.12. Uma vez realizada as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança (CSIRT — Blue Team) da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

1.4.13. Como próximo passo o grupo de resposta a incidente de segurança (CSIRT — Blue Team) da CONTRATADA deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado e quais serão as linhas de atuação para solução do incidente.

1.4.14. O grupo de resposta a incidente de SI (CSIRT — Blue Team) da CONTRATADA deverá definir a severidade do incidente juntamente com o CONTRATANTE. Essa severidade será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente. Mais detalhes sobre definição da severidade se encontra no tópico dos níveis mínimos de serviços.

1.4.15. Após análises iniciais do incidente caberá ao grupo de resposta a incidente de segurança (CSIRT — Blue Team) realizar uma análise mais profunda dos incidentes dos críticos que afetem os critérios de confidencialidade, integridade e disponibilidade, baseando-se no comportamento do ataque e/ou artefato (malware).

1.4.16. Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para esta solução.

1.4.17. Uma vez identificado o comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (CSIRT — Blue Team) da CONTRATADA, deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

1.4.18. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA, através do grupo de resposta a incidente de segurança (CSIRT — Blue Team), inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de análise forense do caso.

1.4.19. Inicia-se então o processo de restauração dos serviços e soluções afetadas gerenciadas pela CONTRATADA, ou seja, a RESPOSTA AO INCIDENTE. Todo este processo é de responsabilidade da CONTRATADA, sendo realizado pelo grupo de resposta a incidente de segurança (CSIRT - Blue Team) da CONTRATADA. As soluções gerenciadas por outrem, deverão ter apoio consultivo para recuperação, caso necessário.

1.4.20. Entende-se como RESPOSTA AO INCIDENTE o restabelecimento do serviço impactado deixando-o operacional para utilização de maneira definitiva ou através de solução de contorno (workaround), sendo que está sempre deverá ser autorizada pelo CONTRATANTE.

1.4.21. Deve-se reunir os dados coletados durante o processo de tratamento de incidente para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança (CSIRT — Blue Team). Tal análise deve ser realizada com o objetivo de identificar pessoas, locais e eventos, correlacionando todas as informações reunidas e gerando como produto um laudo sobre o incidente de segurança em questão. Somente após está analise o incidente deve ser FECHADO.

1.4.22. Caso seja necessário, a reconstrução do ataque deve ser realizada pela CONTRATADA em ambiente controlado, usando-se por exemplo de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da CONTRATADA.

1.4.23. O grupo de resposta a incidente de segurança (CSIRT — Blue Team) da CONTRATADA deve documentar na ferramenta de incidente de segurança as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

1.4.24. Caso a resposta ao incidente não seja efetiva (restabelecimento do serviço) o chamado deve ser reaberto com um nível de criticidade imediatamente superior ao do incidente original.

1.4.25. As ações técnicas adotadas em incidentes de criticidade EMERGENCIAL e ALTA deverão ser revalidadas pelo grupo de resposta a incidente de segurança (CSIRT - Blue Team) em até 18 (dezoito) horas após a RESPOSTA AO INCIDENTE, tal ação caberá a um analista diferente ao que implementou as ações inicialmente. Somente após isso os incidentes destas categorias poderão ser FECHADOS. Caso necessário, a CONTRATADA poderá solicitar a prorrogação do prazo de atendimento, providenciando as devidas justificativas.

1.4.26. No caso da recorrência de um mesmo incidente de criticidade PROBLEMA deverá ser aberto chamado pelo grupo de resposta a incidente de segurança (CSIRT - Blue Team) para que seja feita a devida investigação de sua causa raiz e demais tratativas necessárias à solução definitiva. Neste caso, sua criticidade\SLA será definido como imediatamente superior a dos incidentes que o originaram.

1.4.27. Quando solicitada, a CONTRATADA deverá realizar processos de auditoria e investigação forense, inspecionando logs e informações contidas no SERVIÇO DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO com vistas a rastrear e identificar ações não autorizadas e\ou demais análises que se façam necessárias.

1.4.28. As ferramentas e soluções utilizadas pelo grupo de resposta a incidente de segurança (CSIRT - Blue Team) da CONTRATADA devem ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros.

1.4.29. Espera-se que a linha de base dos eventos de segurança monitorados seja revista de forma mensal, contudo não se limitando a este tempo, pois todos os dias novos ataques são projetados, e se espera que a CONTRATADA tome ciência destes ataques e, por sua vez, atualize a linha de base para que em um cenário onde estes novos ataques sejam direcionados ao CONTRATANTE sejam detectados através dos serviços em questão.

1.4.30. Caso a CONTRATADA identifique a ausência de insumos (logs, eventos ou flows) a ser gerado por um item de configuração, imprescindível a prestação do serviço, será de responsabilidade da CONTRATADA solicitar ao CONTRATANTE a correção e/ou habilitação de tal insumo.

1.4.31. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o CONTRATANTE definiu os seguintes indicadores chaves de desempenho que vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO

Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Incidentes por tipo	Total de incidentes categorizado por tipo	Categoria do incidente	Incidentes	Total de incidentes categorizado por tipo: malware, vazamento de informações., acesso não autorizados., etc.
Incidentes por severidade	Total de incidentes categorizado por severidade	Categoria do incidente	Incidentes	Total de incidentes categorizado por severidade: emergência., alta, média e baixa
Tempo médio resolução	Tempo total das resoluções dividido pelo número de incidentes abertos	Incidentes abertos	Incidentes abertos	Tempo médio para resolução dos incidentes abertos
Tempo médio resposta	Tempo total entre a abertura de um incidente e o início da resposta, dividido pelo total de incidentes abertos	Incidentes abertos	Incidentes abertos	Tempo médio entre a abertura de um incidente e o início da resposta
Downtime para usuários	Soma do downtime dos usuários em minutos	Incidentes abertos	Tempo	Tempo total que os usuários ficaram sem trabalhar por causa dos incidentes
Horas de incidente	Tempo total que a equipe utilizou tratando os incidentes abertos	Incidentes abertos	Tempo	Tempo total que a equipe utilizou tratando os incidentes abertos
Ativos comprometidos	Total de ativos comprometidos categorizado por tipo: servidores, estações, disp. móveis, etc.	Incidentes abertos	Tipo de ativo	Total de ativos comprometidos categorizado por tipo: servidores, estações, disp. móveis, etc.
Investigações forenses	Total de investigações abertas e concluídas	Investigações abertas	Status da investigação	Total de investigações forenses em andamento e concluídas
Quantitativo de incidentes que resultaram em comprometimento da segurança	Soma de incidentes abertos que resultaram em comprometimento da segurança	Incidentes com comprometimento	Incidentes com comprometimento	Número total de incidentes com comprometimento
TOP 10 - IP de destino de incidentes de segurança	Soma do número de incidentes por IP de destino	Incidentes abertos/tratados por IP de destino	IP de destino	TOP do número de incidentes por IP de destino

TOP 10 - Incidentes de segurança por origem	Soma do número de incidentes por origem	Incidentes abertos/tratados por origem	Origem	TOP do número de incidentes por origem interna ou externa
TOP 10 - Tipos de Incidentes	Soma do número de incidentes por tipo	Incidentes abertos/tratados por tipo	Tipo	TOP 10 por tipo de incidente

1.4.32. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Certified Incident Handler), GMON (GIAC Continuous Monitoring) ou profissional com comprovada experiência no tratamento de incidentes de segurança de grande impacto técnico e institucional. Nesse contexto, esse profissional deve apresentá-lo de forma presencial nas dependências da CONTRATADA em Brasília/DF ou de forma virtual, por meio de solução de videoconferência.

1.4.33. Sobre o serviço de gestão de incidentes de segurança, a CONTRATADA deverá monitorar (24x7):

1.4.33.1. Eventos e falhas de segurança conforme sua criticidade por todos os serviços contratados e também nas ferramentas adquiridas pelo CONTRATANTE descritas no " Anexo II - Ambiente Tecnológico ".

1.4.33.2. IOCs.

1.4.33.3. Domínio corporativo.

1.4.33.4. Vazamento de credenciais.

1.4.33.5. Uso indevido ou fraudulento do ativo em websites.

1.4.33.6. Ativo ou expressões similares e nome de domínio na internet.

1.4.33.7. Monitoramento de URLs de redirecionamento para páginas falsas (phishing).

1.4.34. Ademais, a CONTRATADA deve:

1.4.34.1. Criar e ajustar regras de detecção conforme melhores práticas de mercado.

1.4.34.2. Realizar no mínimo dois testes de efetividade por trimestre.

1.4.34.3. Estabelecer plano de resposta a incidentes de segurança.

1.4.34.4. Configurar e sustentar infraestrutura do SIEM.

1.4.34.5. Atender demandas de suporte do SIEM.

1.4.34.6. Elaborar relatório técnicos e gerencias sob demanda.

1.4.34.7. Emitir laudos e relatórios sobre incidentes de segurança.

1.4.34.8. Definir indicadores de desempenho sobre a prestação do serviço.

1.4.34.9. Realizar reuniões técnicas (quinzenal) e gerenciais (mensais).

1.4.34.10. Resolver incidentes em N2 e N3 sob sua responsabilidade.

1.4.34.11. Requisitar apoio para responder à incidentes (CSIRT).

1.4.34.12. As atividades devem ser separadas por níveis, todos contemplados no mesmo serviço aqui descrito.

1.5. MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

1.5.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à ANAC, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em Frameworks de gestão de incidentes (NIST SP 800-61, ISO/IEC 27035 e SANS Incident Handling) e fornecendo como serviço a solução tecnológica Security Information and Event Management (SIEM)

1.5.2. Características gerais da solução SIEM

1.5.2.1. A CONTRATADA deve fornecer o serviço de coleta, análise e correlação de logs, por meio de uma solução de Gerenciamento de Informações e Eventos de Segurança (SIEM).

1.5.2.2. A tecnologia de SIEM a ser implantada deve ter sido homologada e utilizada em outras instituições públicas ou privadas, conforme os documentos de qualificação técnica a serem apresentados pela licitante.

1.5.2.3. Todo hardware e software deve ser fornecido pela CONTRATADA como serviço na vigência do contrato, de acordo com o modelo de disponibilização do serviço, que pode ser em nuvem ou on-premise.

1.5.2.4. A CONTRATADA deverá implantar coletores (virtualizados ou em hardware) no ambiente da ANAC, a fim de realizar a coleta de logs localmente no ambiente da ANAC, absorvendo toda a responsabilidade de implantação dos coletores (Servidores, Máquinas Virtuais, Processamento, Sistema Operacional etc.). a ANAC somente fornecerá energia e link de conexão para o funcionamento da implantação dos coletores.

1.5.2.5. Para a implantação dos coletores, poderá ser aceito o uso de Virtual Appliance da CONTRATADA a ser instalado no ambiente computacional da ANAC, mediante a verificação e aprovação prévias dos requisitos técnicos pela equipe de segurança da informação da ANAC e o atendimento das demais exigências e requisitos apresentados neste Anexo.

1.5.2.6. A ANAC fornecerá conectividade, espaço físico em Rack e energia elétrica (deverá ser compatível com o padrão de tomadas C13) para o funcionamento do hardware e software da solução SàS (Software as a Service).

1.5.2.7. A solução deverá consolidar eventos de log de dispositivos, terminais e aplicativos distribuídos.

1.5.2.8. A solução deverá correlacionar as informações de diferentes fontes de logs e agregar eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes.

1.5.2.9. A solução do processamento de dados transmitidos pelos coletores e executada pela ferramenta SIEM deve ser implementada no modelo totalmente SàS.

1.5.2.10. A solução deverá ter disponibilidade mensal mínima de 99,7%, conforme apresentado no Termo de Referência na Tabela 7.2 - Níveis Mínimos de Serviços Exigidos para o Grupo 01.

1.5.2.11. A solução deve ser flexível a períodos de sazonalidade, permitindo aumento da licença quando necessário e retorno ao volume inicial contratado quando o período de sazonalidade finalizar. De acordo com o volume de eventos, poderão ser solicitados pacotes adicionais de EPS, correspondentes ao item 6, os quais deverão ser disponibilizados em até 1 mês da data de solicitação.

1.5.2.11.1. A solução deve possibilitar a recepção de eventos que temporariamente ultrapassem os limites contratados. O volume excedente será processado assim que o volume for normalizado, funcionando com picos temporários sem perder eventos ou incorrer em cobranças adicionais por excesso.

1.5.2.11.2. A cobrança sobre o volume sazonal será realizada conforme o volume de Eventos por Segundo (EPS) tratado.

1.5.2.12. Para as soluções que utilizem a métrica de GB/dia (gigabytes por dia), deverá ser observada a proporção de 512 byes por evento, para fins de comparação.

1.5.2.13. As soluções que utilizem como métrica a quantidade de dispositivos deverão considerar os parâmetros constantes do anexo “AMBIENTE TECNOLÓGICO DA ANAC” para seu dimensionamento.

1.5.3. A solução deverá possibilitar a coleta dos logs on-premise, o que poderá ocorrer por meio do uso de agentes ou sem agentes.

1.5.4. Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM.

1.5.5. Quando coletando logs que estão hospedados na nuvem, a coleta deve ocorrer diretamente da nuvem da aplicação para a nuvem do SIEM, sem permitir que os logs passem pela infraestrutura da ANAC. Isso é válido desde que a solução em nuvem permita a coleta por meio de integrações via API. Qualquer questionamento de serviços em nuvem usados pela ANAC poderá ser esclarecido na Vistoria Técnica.

1.5.6. A solução deverá segregar logicamente os logs da ANAC dos demais logs de outras contratantes que utilizem a solução de SIEM SàS na infraestrutura da CONTRATADA.

1.5.7. A solução deve ser monitorada para garantir disponibilidade e infraestrutura em tempo integral, 24 horas por dia, 7 dias por semana, durante todo o ano.

1.5.8. Se a solução consistir em módulos, eles devem ser fornecidos por um único fabricante para garantir suporte completo em relação a funcionalidades, integrações e compatibilidade de 100% com a solução. Como um dos requisitos da ferramenta SIEM para a assinatura do TRD de implantação, a CONTRATADA deverá apresentar documentação fornecida pelo fabricante para comprovar a cobertura de garantia do fabricante relacionada com a funcionalidade da ferramenta SIEM.

1.5.9. A solução deve armazenar os logs por pelo menos 6 meses online.

1.5.10. O armazenamento dos logs deve ser efetuado no território brasileiro pela CONTRATADA. Os logs poderão trafegar por território fora do Brasil, desde que obedecidos os critérios do Capítulo V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS - da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

1.5.11. A coleta, normalização e correlacionamento dos eventos dos dispositivos monitorados devem ocorrer em tempo próximo ao real.

1.5.12. A fim de aprimorar a operação e a compreensão dos eventos, é obrigatório normalizá-los e categorizá-los em um único padrão que será utilizado pela solução.

1.5.13. A solução deve possibilitar a criação de metadados personalizados, permitindo a extração de dados existentes na linha de log (raw). Isso pode ser realizado por meio de recursos como expressões regulares ou interfaces gráficas dedicadas para essa finalidade.

1.5.14. Propriedades customizadas poderão ser utilizadas em regras de correlação online e histórica.

1.5.15. A solução deve possibilitar a agregação de eventos similares.

1.5.16. A solução deve atribuir uma métrica de prioridade tanto para os eventos quanto para os alertas/incidentes.

1.5.17. A solução deve ser capaz de gerar alertas/incidentes com base em regras predefinidas anteriormente.

1.5.18. A solução deve ter a capacidade de armazenar os eventos, incluindo aqueles normalizados, de forma compactada.

1.5.19. A solução deve possibilitar a análise de eventos com base em contexto, como usuários, localização geográfica e qualquer outro metadado presente nos eventos.

1.5.20. A solução deve fornecer painéis gráficos ou integração com painéis gráficos existentes na ANAC (dashboards), que apresentam indicadores de segurança, aplicações e monitoramento do SIEM.

1.5.21. Os painéis gráficos (dashboards) devem ser personalizáveis por usuário, permitindo a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução na interface web.

1.5.22. O Dashboard integrado deve:

1.5.22.1. Fornecer um painel que apresente uma visão consolidada das métricas de segurança dos ativos monitorados.

1.5.22.2. Permitir a personalização do painel, incluindo a adição de relatórios e métricas.

1.5.22.3. Realizar a análise dos eventos de segurança da informação em quase tempo real.

1.5.22.4. Assegurar a funcionalidade de análise por meio do drill-down, possibilitando a exploração detalhada a partir de um gráfico de visão geral, com a capacidade de descer aos diferentes níveis de análise conforme necessário.

1.5.22.5. Permitir minimamente o acesso de leitura para a equipe da ANAC em qualquer momento.

1.5.23. Ter a capacidade de enviar e-mails ou mensagens via SMS contendo notificações sobre incidentes ou alertas.

1.5.24. A solução deve oferecer, no mínimo, os seguintes métodos de coleta de eventos: Syslog (UDP, TCP), Syslog com criptografia TLS, JDBC, SNMP (v1, v2 e v3), Registro de Eventos do Microsoft, Cliente MQ Series, Arquivos de Log em formato de texto, Kafka, Checkpoint OPSEC/LEA.

1.5.25. A solução deve ser capaz de encaminhar os logs e fluxos, em seu formato nativo, para outros sistemas de segurança da informação ou servidores Linux/Windows em tempo real.

1.5.26. A solução deve ser capaz de encaminhar eventos já normalizados para outros sistemas de correlação em tempo real.

1.5.27. A solução deve oferecer a capacidade de configurar a ofuscação de qualquer parte dos dados recebidos após a normalização. A configuração da ofuscação de dados deve ser realizada por meio de chaves de criptografia.

1.5.28. A solução deve ser capaz de automatizar a resposta a incidentes, executando scripts como ação personalizada dentro das regras de correlação.

1.5.29. A solução deve permitir a personalização e customização de diversos modelos de e-mail que serão enviados como resposta aos incidentes identificados.

1.5.30. A solução deve ser capaz de processar logs no formato JSON, identificando e criando automaticamente os campos comuns do log como metadados para aquele tipo de log.

1.5.31. A solução deve permitir a criação de metadados com nomes personalizados, à escolha do administrador, e possibilitar a referência desses metadados em pesquisas e regras de correlação.

1.5.32. A solução deve permitir a personalização/definição de metadados para extrair dados de uma linha de log (raw), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, possibilitando o uso desses dados em pesquisas de eventos.

1.5.33. Características do coletor de logs do SIEM

1.5.33.1. A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de preferência (network appliance ou virtualização), desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos da ANAC.

1.5.33.2. Os coletores deverão comunicar-se com o SIEM da CONTRATADA através de VPN com tráfego criptografado.

1.5.33.3. Deverá possibilitar a compressão/compactação e criptografia dos dados para o envio dos logs à nuvem.

1.5.33.4. Deverá realizar a filtragem e seleção dos eventos a serem inseridos na solução ou mantidos na base de dados da solução, conforme períodos definidos previamente.

1.5.33.5. Deverá possibilitar a criação e modificação de políticas de retenção.

1.5.33.6. Deverá realizar a normalização e categorização dos eventos em um padrão único, que será utilizado pela solução.

1.5.33.7. Deverá oferecer suporte nativo para o reconhecimento e coleta de pelo menos 250 tipos distintos de fontes de dados.

1.5.33.8. Deverá processar eventos em formato comprimido (zip, gz, tar.gz) sem exigir descompressão manual.

1.5.33.9. Deverá realizar a agregação de eventos, exibindo a contagem de ocorrências quando o mesmo evento acontecer dentro de um período curto.

1.5.33.10. A possibilidade de efetuar a agregação de eventos deve ser configurável, permitindo escolher entre realizar ou não essa operação.

1.5.33.11. Deverá preservar o evento bruto (raw), juntamente com seus metadados para fins de armazenamento e consultas futuras.

1.5.33.12. Deverá ter a capacidade de agregar informações de localização geográfica dos endereços IP envolvidos no evento, a fim de utilizá-las na correlação.

1.5.33.13. A solução deve ter a capacidade de coletar, processar e normalizar tanto os eventos de segurança quanto os eventos de negócio (não relacionados à segurança).

1.5.33.14. Os eventos de segurança e de negócios devem ser normalizados para um único padrão de eventos.

1.5.33.15. A solução deve oferecer suporte à integração de dispositivos ou logs que não são nativamente suportados.

1.5.33.16. A integração de logs ou dispositivos deve ser feita através da interface web, utilizando expressões regulares, JSON e recursos similares, sem definir de maneira obrigatória a utilização de linguagens de programação ou scripts, como Java, C, TCL/TK, PowerShell, Shell Scripts, entre outros.

1.5.33.17. A integração mencionada deve ser compatível com as seguintes formas de coleta de eventos:

1.5.33.17.1. Check Point OPSEC/LEA.

1.5.33.17.2. Kafka.

1.5.33.17.3. Arquivos de Log em Formato de texto.

1.5.33.17.4. Syslog (UDP, TCP).

1.5.33.17.5. Microsoft Event Log.

1.5.33.17.6. Juniper NSM Protocol.

1.5.33.17.7. SNMP (v1, v2 e v3).

1.5.33.17.8. CISCO NSEL.

1.5.33.17.9. Syslog criptografado com TLS.

1.5.33.17.10. PAN-OS XML

1.5.33.17.11. Common Event Format (CEF)

1.5.33.17.12. Outros formatos de logs presentes nos ativos de rede da ANAC (switches, access point, etc.).

1.5.33.18. A solução precisa ter suporte incorporado para, no mínimo, as seguintes fontes de logs:

1.5.33.18.1. Windows.

1.5.33.18.2. Linux.

1.5.33.18.3. Oracle Database.

1.5.33.18.4. PostgreSQL.

1.5.33.18.5. MS SQL Server.

1.5.33.18.6. Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet, Palo Alto e SonicWall).

1.5.33.18.7. Network IPS/IDS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee).

1.5.33.18.8. Outras fontes de logs de tecnologias presentes na infraestrutura da ANAC.

1.5.33.19. A solução deve oferecer a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, a partir das opções nativamente suportadas e enviadas via Syslog.

1.5.33.20. A solução deve ter a capacidade de criar automaticamente data sources com base na detecção do tipo de fonte de log, incluindo tipos de logs personalizados na solução, quando enviados via Syslog.

1.5.33.21. A solução deve ter suporte para IP overlap, ou seja, categorizar os eventos de forma que seja possível gerenciar eventos provenientes de fontes de log que estão em redes distintas, mas possuem o mesmo endereço IP.

1.5.34. Recursos de correlação de logs do SIEM.

1.5.34.1. Considera-se tempo de processamento "quase real" no receptor, ao processamento instantâneo da informação mais o atraso de tráfego de dados entre o emissor e o receptor.

1.5.34.2. A solução deve realizar a correlação de eventos provenientes das fontes de logs e flows, resultando na geração de incidentes de segurança.

1.5.34.3. A solução deve efetuar a correlação dos eventos em tempo quase real.

1.5.34.4. A solução deve efetuar a correlação dos flows em tempo quase real.

1.5.34.5. A solução deve oferecer a capacidade de criar regras inexistentes e editar as existentes.

1.5.34.6. A solução deve permitir a correlação de qualquer informação presente no evento, inclusive dados financeiros ou outras informações que não estejam relacionadas a endereçamento IP, portas etc.

1.5.34.7. Oferecer um mínimo de 150 regras incorporadas, permitindo a criação ilimitada de novas regras ou personalização das regras incorporadas:

1.5.34.7.1. Ataques de força bruta com e sem sucesso.

1.5.34.7.2. Detecção de anomalias de comportamento baseado em estatísticas (Statistical Behavioral Analysis).

1.5.34.7.3. Infecção de equipamentos por vírus.

1.5.34.7.4. Comprometimento ou invasão de ativos da rede.

1.5.34.7.5. Anomalias de Logon: excessivas falhas de logon, logons fora do expediente, logons a partir de endereços IP não usuais.

1.5.34.7.6. Realização de ações suspeitas por parte de usuários privilegiados.

1.5.34.7.7. Detecção de padrões em logs observados e não observados.

1.5.34.7.8. Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade).

1.5.34.7.9. Bloqueio de contas e password scans.

1.5.34.7.10. Ataques comuns em aplicações WEB, como XSS e SQL injection.

1.5.34.7.11. Ataques de negação de serviço (DoS e DDoS).

1.5.34.7.12. Identificação em tempo real e de maneira automatizada da origem dos eventos de segurança, identificando cidades, estados e países e não somente os endereços IP de origem.

1.5.34.7.13. Botnets, worms, DDoS e outros zero-day malwares, através do cruzamento dos logs de DNS, DHCP, web proxy e tráfego de rede.

1.5.34.8. As regras podem variar desde a detecção simples de thresholds até o uso de operadores lógicos comuns para correlacionar eventos distintos, possibilitando:

1.5.34.8.1. Permitir a utilização de thresholds estáticos ou dinâmicos.

1.5.34.8.2. Facilitar a execução de scripts automáticos em casos de incidentes.

1.5.34.8.3. Permitir a configuração de políticas de notificação com base na severidade do incidente, hora do dia e serviço.

1.5.34.8.4. Integrar a solução com a monitoração de capacidade e desempenho dos ativos gerenciados via SNMP.

1.5.34.9. A capacidade de autodetecção deve incluir:

1.5.34.9.1. Oferecer recursos mínimos de busca de eventos, incluindo: busca em tempo real utilizando palavras-chave semelhantes ao Google e consultas estruturadas semelhantes ao SQL, assim como ter a capacidade de converter os resultados da busca em relatórios ou widgets de painel.

1.5.34.9.2. A solução deve incluir regras de correlação específicas para regulamentações e conformidades aplicáveis à ANAC, com suporte mínimo para PCI, ISO 27001 e GDPR ou LGPD.

1.5.34.9.3. A solução deve possuir um repositório que ofereça novas regras de correlação especializadas em segurança para atualização e expansão da capacidade de detecção de incidentes, sem custos adicionais.

1.5.34.9.4. A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surtos ou ausência de eventos/tráfego, quando comparados a períodos semelhantes (por exemplo, mesmo período do dia, mesmo dia da semana).

1.5.34.9.5. A solução deve permitir a criação de regras que identifiquem desvios em qualquer metadado, em relação aos limites preestabelecidos.

1.5.34.9.6. A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que ocorrem ao longo do tempo e não foram previstos ou observados anteriormente.

1.5.34.9.7. A solução deve integrar-se minimamente com pelo menos uma das ferramentas externas como Nslookup, Whois e Nmap.

1.5.34.9.8. A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas de observação (watchlist), permitindo também a criação e edição automatizada e manual de listas.

1.5.34.9.9. A solução deve ser capaz de correlacionar eventos de pelo menos um dos fluxos de rede, como NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução.

1.5.34.9.10. A solução deve ser capaz de correlacionar eventos provenientes de múltiplas fontes, tipos ou localizações.

1.5.34.9.11. A solução deve ter a capacidade de priorizar os eventos e incidentes com base em critérios que incluem, pelo menos, severidade e criticidade/relevância do evento ou incidente. Deve ser possível utilizar uma combinação desses critérios para determinar a prioridade.

1.5.34.10. Os incidentes devem ser agrupados, no mínimo, de acordo com:

1.5.34.10.1. Endereço de origem.

1.5.34.10.2. Endereço de destino.

1.5.34.10.3. Categoria.

1.5.34.11. A solução deve ter, no mínimo, os seguintes tipos de correlação:

1.5.34.11.1. Extrapolação de um limite (threshold).

1.5.34.11.2. Correlação por anomalia e padrão de comportamento.

1.5.34.11.3. Correlação por regras.

1.5.34.12. Como resultado das regras, a solução deve ter a capacidade de realizar ações automáticas, no mínimo:

1.5.34.12.1. Enviar e-mail.

1.5.34.12.2. Enviar mensagens para o usuário conectado no console.

1.5.34.12.3. Criar um incidente no sistema de workflow interno.

1.5.34.12.4. Enviar traps SNMP e popular listas (watchlist).

1.5.34.13. A solução deve possuir a capacidade de se integrar com os principais sistemas de inteligência de ameaças de riscos globais ou, no mínimo com o do próprio fabricante, além das soluções de segurança da informação presente na ANAC conforme item 1.1. Soluções de segurança do Anexo X - "Anexo II - Ambiente Tecnologico.pdf".

1.5.34.14. A solução deve oferecer a flexibilidade de utilizar qualquer metadado dos eventos em regras de correlação.

1.5.34.15. A solução deve permitir testar as regras de correlação em eventos passados, com um período de tempo e escopo claramente definidos.

1.5.34.16. A correlação histórica deve fornecer a opção de escolher o período a ser analisado, com suporte mínimo para correlação de 1 dia, 7 dias e 30 dias.

1.5.34.17. As regras de correlação histórica devem processar logs e flows, gerando alertas quando os eventos/flows analisados corresponderem às especificações definidas na regra.

1.5.34.18. Uma regra de correlação deve ter a capacidade de correlacionar eventos de tipos e origens distintos, verificando situações como a sequência de eventos diferentes, a contagem de eventos e a ausência de um evento após a ocorrência de outro.

1.5.35. Recursos da console de administração e operação do SIEM.

1.5.35.1. A console de administração e operação deve ser configurada e operada pela CONTRATADA.

1.5.35.2. A console de consulta deve incluir a capacidade de classificar os eventos em geral em três grupos distintos:

1.5.35.2.1. Eventos de auditoria (logins, logouts, erros de autenticação etc.).

1.5.35.2.2. Eventos de Segurança (ataques, comprometimento, roubo de dados, fraudes etc.).

1.5.35.2.3. Eventos de Operação (erros, eventos críticos de ativos e rede etc.).

1.5.35.3. A console deve contar com as seguintes especificações:

1.5.35.3.1. Ter uma interface web única, via HTTPS, para administração, gerenciamento e operação do sistema como um todo, garantindo a confidencialidade dos dados.

1.5.35.3.2. Ter acesso controlado e autenticado por usuário.

1.5.35.3.3. Ter capacidade de integração com pelo menos duas das seguintes bases: Microsoft Active Directory, LDAP, TACACS ou RADIUS para autenticação de usuários.

1.5.35.3.4. Garantir acesso aos dados e funcionalidades específicas por perfis de usuário.

1.5.35.3.5. O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução de acordo com os perfis de usuários definidos pelo administrador.

1.5.35.3.6. O controle de acesso deve ser configurado para permitir o acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, atividades de Redes e Logs.

1.5.35.3.7. Permitir a visualização de pelo menos dois dos seguintes itens: de eventos, flows de rede e incidentes de segurança em tempo quase real.

1.5.35.3.8. Permitir a pesquisa nos eventos históricos com base em metadados, oferecendo a capacidade de drill-down, ou seja, refinamento da pesquisa a partir da seleção de elementos no resultado para realizar uma nova pesquisa.

1.5.35.3.9. Disponibilizar a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

1.5.35.3.10. A solução deve permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução.

1.5.35.3.11. Ter a capacidade de criar novos painéis gráficos (dashboards) e modificar os existentes.

1.5.35.3.12. Ter a capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (exemplo: Firewall, Proxy e antivírus na mesma visualização).

1.5.35.3.13. Ter a capacidade de criar listas (watchlist) e alterar as existentes, permitindo a inserção dos dados de forma manual, por linha de comando e automática por meio das regras de correlação.

1.5.35.3.14. Permitir a remoção de dados das listas (watchlist) de forma manual, automática por meio das regras de correlação e por expiração do tempo de vida da informação.

1.5.35.3.15. Possuir a capacidade de gerenciar e configurar centralmente todas as partes distribuídas da solução.

1.5.35.3.16. Possuir a capacidade de atualizar os componentes da solução.

1.5.35.3.17. Caso a solução seja on-premise, deve ter a capacidade de restaurar informações de cópia de segurança do banco de dados, configurações e dados que foram arquivados previamente pela solução.

1.5.35.3.18. Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente.

1.5.35.3.19. Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes ou definidos pelo usuário.

1.5.35.3.20. Deve oferecer APIs do tipo webservices, seguindo o padrão "RESTful API", para permitir o acesso externo à solução, possibilitando a busca de informações de eventos e flows, assim como a manipulação de incidentes.

1.5.35.3.21. Deve suportar o controle de acesso à solução com base em informações externas, validando atributos do usuário ou grupo a que ele pertence. Essa validação de autorização deve ser suportada em diretórios LDAP ou Windows Active Directory.

1.5.35.3.22. Deve fornecer uma API para a criação de fontes de logs (data sources) por meio de uma interface ReST, com o objetivo de automatização.

1.5.35.4. Os relatórios devem contar com as seguintes especificações:

1.5.35.4.1. Deve permitir a geração de relatórios, em quase tempo real, que englobem diversas informações em um único documento, como dados de segurança e rede.

1.5.35.4.2. Fornecer a funcionalidade de geração de relatórios de conformidade, abrangendo, pelo menos, SOX, PCI e ISO.

1.5.35.4.3. Deve ser permitido agendar a execução de relatórios em qualquer horário ou período, com a opção de enviar os resultados por e-mail.

1.5.35.4.4. Deve permitir a criação de relatórios relacionados a incidentes em pelo menos duas das seguintes fontes: logs, flows de rede e vulnerabilidades.

1.5.35.4.5. Deve organizar os relatórios em grupos temáticos, permitindo a criação de novos agrupamentos de relatórios pelos usuários.

1.5.35.4.6. Deve possibilitar a personalização de novos relatórios com base em pelo menos duas das seguintes fontes: dados de Logs, Flows de rede, Vulnerabilidades e Incidentes.

1.5.35.4.7. Deve gerar relatórios de eventos, alertas/incidentes em níveis técnico e gerencial, que podem ser exportados nos formatos PDF, XLS, CSV, ou DOC.

1.5.35.4.8. Os usuários devem ter acesso apenas aos seus próprios relatórios ou aos relatórios disponibilizados por outros usuários. Os administradores devem ter acesso a todos os relatórios.

1.5.35.4.9. Caso a solução seja on-premise, deve ser possível definir perfis de usuários com permissões/restrições para editar os modelos de relatórios.

1.5.35.4.10. Caso a solução seja on-premise , a funcionalidade de backup deve preservar os dados dos relatórios.

1.5.35.4.11. Deve permitir a geração de relatórios que incluam os eventos associados a um incidente detectado por regras de correlação.

1.5.35.4.12. Permitir classificar eventos de segurança: ataques, reconhecimento, malware, atividades suspeitas de rede ou usuários etc.

1.5.35.4.13. Contar com a opção de incluir os TOP endereços lógicos de origem das ameaças, TOP países e cidades de origem das ameaças e dos alertas de segurança.

1.5.35.5. A CONTRATADA deverá garantir que terá acesso ao suporte do fabricante da tecnologia SIEM durante a vigência do contrato. Para isso, a CONTRATADA deverá apresentar um acordo de suporte direto com o fabricante, assegurando que terá acesso a especialistas qualificados para resolver dúvidas, consultas ou problemas de configuração relacionados à ferramenta SIEM.

1.5.36. Dimensionamento do SIEM.

1.5.36.1. A CONTRATADA deve fornecer o serviço de solução SIEM com funcionamento de 3.000 EPS por 24 meses a partir do TRD de implantação.

1.5.36.2. Como estratégia de complementação de EPS, a CONTRATADA deve oferecer a possibilidade de fornecer até 10 pacotes adicionais, usados sob demanda, de 500 EPS cada um. Os pacotes adicionais podem ser demandados de forma gradual e seu quantitativo poderá variar em virtude da flutuação natural do tamanho da rede durante a execução contratual. Portanto, os quantitativos de pacotes de EPS contratados representam meramente uma estimativa de utilização de serviço. Não haverá obrigação da ANAC na utilização do quantitativo parcial ou total dos pacotes extras. Somente serão devidos e pagos os pacotes adicionais efetivamente prestados e demandados através das respectivas Ordens de Serviço. A quantidade de pacotes adicionais demandados pode ser redimensionado em qualquer momento para quantidades maiores ou anualmente em quantidade menor (dentro da duração do contrato) e em função da mudança de monitoramento demandado pela ANAC.

1.5.36.2.1. Para as soluções que utilizem a métrica de GB/dia (gigabytes por dia), deverá ser observada a proporção de 512 byes por evento, para fins de comparação.

1.5.36.2.2. As soluções que utilizem como métrica a quantidade de dispositivos deverão considerar os parâmetros constantes do anexo “AMBIENTE TECNOLÓGICO DA ANAC” para seu dimensionamento.

1.5.37. Serviço de monitoramento e correlação de eventos de segurança da informação

1.5.37.1. As atividades do Serviço de monitoramento e correlação de eventos de segurança da informação serão medidas por Níveis Mínimos de Serviço.

1.5.37.2. Os profissionais alocados no serviço de monitoramento e correlação de eventos (Analista SIEM) serão integrantes das operações no SOC.

1.5.37.3. A CONTRATADA deverá disponibilizar, nas instalações da ANAC (Brasília/DF), o acesso de leitura a console das tecnologias que suportam os serviços de Gestão de Vulnerabilidades e de Coleta, Análise e Correlação de Logs (SIEM).

1.5.37.4. Dimensionamento de EPS por tipo de equipamento na rede da ANAC e futuras expansões ou modificações.

1.5.37.5. Monitoramento 24x7x365 da infraestrutura de TI, utilizando a ferramenta SIEM como sua tecnologia base.

1.5.37.6. A CONTRATADA deverá adotar uma abordagem preventiva e reativa, identificando eventos suspeitos, classificando os incidentes de cibersegurança e fornecendo à ANAC um relatório para cada evento identificado.

1.5.37.7. A CONTRATADA terá a responsabilidade de identificar e classificar os eventos de segurança utilizando a ferramenta de SIEM. O Blue Team

(responsável pela execução do Item 4 – Gestão de incidentes de segurança da informação), com apoio do serviço de monitoramento, será responsável por tratar o evento no serviço/host indicado no relatório fornecido pela CONTRATADA.

1.5.37.8. O serviço de SIEM deverá oferecer à ANAC as seguintes facilidades:

1.5.37.8.1. Monitoração de correlação de eventos.

1.5.37.8.2. Gestão de incidentes.

1.5.37.8.3. Criação de novas regras de correlação e casos de uso e detecção.

1.5.37.8.4. Inteligência de ameaças e conformidade.

1.5.37.9. Triagem de incidentes identificados pelo serviço de monitoramento.

1.5.37.9.1. É necessário realizar uma triagem inicial nos chamados abertos pela monitoração de segurança, identificando e agrupando os potenciais incidentes que possuam características semelhantes, como ataques direcionados ao mesmo servidor, ataques originados do mesmo IP ou múltiplas falhas de login, por exemplo.

1.5.37.9.2. Após a etapa de triagem inicial, os chamados devem ser avaliados para determinar se são resultantes de falsos positivos/negativos, além disso, serão realizados testes para verificar a veracidade do incidente detectado.

1.5.38. Problemas identificados pelo serviço de monitoramento.

1.5.38.1. A equipe da CONTRATADA deve abrir chamados de problema em seu próprio sistema e no sistema da ANAC, relacionados ao serviço de monitoração, a fim de identificar a causa raiz. O Blue Team, com o suporte do serviço de monitoramento, deve solucionar o(s) problema(s) identificado(s) ao atender as demandas de incidentes.

1.5.38.2. Os chamados devem ser atendidos pelo Blue Team, com o apoio do serviço de monitoramento.

1.5.39. Incidentes de segurança identificados pelo serviço de monitoramento.

1.5.39.1. O Blue Team, com o suporte do serviço de monitoramento, será responsável por lidar com todo tipo de incidente e executar os procedimentos de resposta para que seja implementada a respectiva solução.

1.5.39.2. A ANAC deve ser notificada sobre os incidentes por meio do sistema de chamados, e-mail e/ou telefone, conforme acordado previamente com a ANAC, de acordo com as necessidades de comunicação interna e/ou externa.

1.5.39.3. A CONTRATADA deve fornecer informações sobre os incidentes à ANAC, por meio da abertura de chamados na ferramenta de ITSM da ANAC.

1.5.40. Ocorrência de Incidentes no serviço de monitoramento.

1.5.40.1. Em caso de detecção de algum incidente de segurança, a CONTRATADA deve contatar imediatamente a ANAC por telefone, e- mail e abertura de chamado na ferramenta de ITSM da ANAC. Isso é necessário para que sejam tomadas as medidas corretivas e legais adequadas, tanto pela equipe da CONTRATADA quanto, se necessário, com a colaboração da equipe da ANAC, seguindo o procedimento estabelecido para resposta a incidentes.

1.5.40.2. O serviço de monitoramento deve comunicar imediatamente à ANAC sobre acessos indevidos, instalação de códigos maliciosos ou qualquer outra

ação que represente um risco para a segurança do ambiente da ANAC. Isso deve ser feito mesmo se essas tentativas não forem bem-sucedidas, mas houver persistência por parte do agente mal-intencionado.

1.5.40.3. O serviço de monitoramento deve fornecer todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs etc.) para que os incidentes de segurança relatados possam ser investigados pelo Blue Team, com o suporte do serviço de monitoramento.

1.5.41. Resposta a incidentes no serviço de monitoramento.

1.5.41.1. A CONTRATADA deve incluir as informações necessárias, como origem do ataque, tipo de ataque, data e hora, logs, causa do incidente de segurança e o procedimento de resposta ao incidente na ferramenta de ITSM da ANAC, a fim de possibilitar a implementação das medidas corretivas necessárias pelo Blue Team, com o suporte do serviço de monitoramento.

1.5.41.2. Os incidentes de segurança devem estar relacionados a eventos de segurança das soluções monitoradas e podem incluir, mas não se limitar a, acessos indevidos, instalações de códigos maliciosos, indisponibilidade de serviços devido a ataques de negação de serviço (DoS e DDoS), ataques por força bruta ou qualquer outra ação que possa comprometer a confidencialidade, disponibilidade ou integridade das informações da ANAC.

1.5.42. Software e Hardware necessários para a solução SIEM no serviço de monitoramento.

1.5.42.1. A CONTRATADA é responsável por fornecer os softwares e hardwares necessários para implantar os serviços gerenciados de monitoramento e correlação de eventos de segurança da informação, durante o prazo do contrato e sem custos adicionais para a ANAC.

1.5.43. Configuração do Security Information and Event Management (SIEM).

1.5.43.1. A CONTRATADA deverá ativar o serviço que será utilizado como ferramenta, durante a vigência do contrato e antes do TRD de implantação, para prestação do Serviço de Coleta, Análise e Correlação de Logs, através de uma solução SIEM.

1.5.43.2. A CONTRATADA deve realizar a implementação das configurações, regras e políticas apropriadas para o ambiente da ANAC, levando em consideração as necessidades específicas do ambiente.

1.5.43.3. A ANAC, com o suporte da CONTRATADA, será responsável por realizar as configurações nos equipamentos de rede (switches, roteadores, servidores etc.), servidores Linux/Windows e equipamentos de segurança da informação da ANAC para enviar os logs para a solução de SIEM. Adicionalmente, as configurações na solução de SIEM são de responsabilidade da CONTRATADA.

1.5.43.4. As configurações, regras de correlação, alertas e outras configurações do SIEM serão implementadas pela CONTRATADA e de propriedade intelectual e responsabilidade exclusiva da ANAC. Portanto, essas configurações não devem ser extraídas, copiadas, manipuladas ou removidas sem o consentimento expresso da ANAC.

1.5.43.5. A Solução de SIEM deve abrir automaticamente chamados na ferramenta de ITSM da ANAC sempre que detectar um possível incidente de disponibilidade ou segurança.

1.5.43.5.1. Não sendo possível a integração entre a solução de SIEM e de ITSM, o registro dos chamados deverá ser realizado manualmente.

1.5.43.6. Toda a mão de obra especializada necessária para a instalação e configuração da solução de SIEM deve ser fornecida pela CONTRATADA.

1.5.43.7. A CONTRATADA é responsável por executar todas as operações de monitoramento, gerenciamento e administração da solução de SIEM, conforme determinação da ANAC, abrangendo, mas não se limitando a:

1.5.43.7.1. Coleta de logs.

1.5.43.7.2. Criação de regras de correlação, não havendo limite mínimo para qualquer ativo e obrigatoriamente tratando todos os ativos monitorados.

1.5.43.7.3. Realização de configurações do SIEM (agentes, regras de incidentes, regras de correlação etc.).

1.5.43.7.4. Interação com o fabricante da solução.

1.5.43.7.5. Backup e restore.

1.5.43.7.6. Resolução de problemas.

1.5.43.7.7. Suporte.

1.5.43.7.8. Instalação de serviços relativos ao escopo contratado.

1.5.43.7.9. Atualização, de acordo com as recomendações do fabricante.

1.5.43.7.10. Demais operações citadas anteriormente.

1.5.43.8. Durante a fase de implantação, a CONTRATADA deve apresentar um conjunto de regras pré-definidas para ativação. Essas regras só serão implementadas após a aprovação da ANAC.

1.5.43.9. A CONTRATADA será responsável por documentar as regras aprovadas pela ANAC. A documentação de regras aprovadas (novas ou atualizadas) deve seguir os processos de gerenciamento de mudanças da ANAC.

1.5.43.10. A ANAC tem permissão para solicitar alterações nas regras de correlação de eventos, de forma a ajustá-las às suas necessidades. Tais alterações serão devidamente solicitadas via abertura de chamado.

1.5.43.11. A CONTRATADA deverá prestar todos os serviços relativos ao SIEM (implantação, configuração, manutenção, análise de logs, detecção/resposta a incidentes, backup e restore etc.), conforme requisitos de funcionamento do SIEM.

1.5.43.12. A operação da console de administração e operação deverá ser de responsabilidade exclusiva da CONTRATADA.

1.5.43.13. É de responsabilidade da CONTRATADA realizar a integração do SIEM de forma a possibilitar o recebimento de alertas e a abertura automática de incidentes na ferramenta de ITSM da ANAC.

1.5.44. Perfil dos profissionais.

1.5.44.1. Devem possuir graduação em cursos de tecnologia da informação e contar com experiência comprovada (CTPS, contrato de Pessoa Jurídica), no cargo a ser executado, de no mínimo 12 meses.

1.5.44.2. Deve contar com a certificação relacionada e emitida pelo fabricante da ferramenta SIEM usada no serviço de monitoramento e correlação de eventos.

1.5.44.3. Deve contar com proficiência de inglês intermediário para poder estabelecer comunicação com a comunidade técnica do fabricante da ferramenta SIEM, com o objetivo de obter informações que ajudem na implantação, execução, configuração e manutenção da ferramenta SIEM.

1.5.44.4. Deve contar com especialização em segurança da informação, comprovada através de certificado de conclusão ou diploma emitido por instituição de ensino superior reconhecida pelo Ministério da Educação ou com, pelo menos, uma das seguintes certificações: CompTIA Security+. EXIN Information Security Foundation. EXIN Ethical Hacking Foundation. GIAC Security Essentials (GSEC).

1.6. GESTÃO DE VULNERABILIDADES

1.6.1. O serviço de Gestão de Vulnerabilidades (item 7 da Tabela 1.1 do TR) poderá ser realizada remotamente e terá como objetivo principal a análise geral do ambiente da CONTRATANTE quanto a segurança da informação para identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica da CONTRATANTE, bem como apresentar recomendações de melhorias e/ou correções das vulnerabilidades identificadas durante os testes.

1.6.2. Fazem parte do processo de gestão de vulnerabilidades as fases de varredura de vulnerabilidades, alerta de Vulnerabilidades e Controle das vulnerabilidades. Estas fases devem atuar de forma integrada com o objetivo de proverem informações suficientes para uma proteção mais eficaz do ambiente da CONTRATANTE.

1.6.3. A periodicidade da execução das fases supracitadas dentro da vigência contratual deverá seguir as exigências dos itens a seguir.

1.6.4. Características gerais

1.6.4.1. A empresa CONTRATADA deverá entregar ao gestor do contrato, ou técnico indicado por ele, todo detalhamento dos testes, sejam manuais ou automatizados, a serem realizados, desde os ativos a serem testados, qual procedimento adotado, ferramentas utilizadas, entre outras informações que possam ser solicitadas.

1.6.4.2. Os testes de infraestrutura só poderão acontecer mediante autorização do gestor técnico do contrato, ou técnico indicado por ele.

1.6.4.3. Os testes de sistemas só poderão acontecer mediante autorização do gestor técnico do contrato, ou técnico indicado por ele, com anuência da área técnica responsável pela sustentação em produção do sistema do escopo.

1.6.4.4. Todos os testes a serem realizados deverão ser precedidos de caderno de testes, contendo todo o detalhamento das ações a serem executadas, possíveis comprometimentos, possíveis ações de contorno, dentre outras informações que se julguem necessárias para garantia da segurança e do sigilo das informações da CONTRATANTE.

1.6.4.5. Todas as fases dos testes serão acompanhadas e supervisionadas a critério da CONTRATANTE.

1.6.4.6. Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverão ser reportadas, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

1.6.5. Varredura de vulnerabilidades

1.6.6. Deverá ser realizada mensalmente uma varredura interna de vulnerabilidades no escopo descrito abaixo.

1.6.6.1. Levantamento de todos os ativos da infraestrutura que deverão ser alvo da varredura. Para cada ativo, deverão ser levantados além das informações básicas, as informações de criticidade do ativo no ambiente e as informações das janelas de manutenção e mudança caso seja necessário aplicar patch e/ou correções.

1.6.6.2. Execução da varredura de vulnerabilidades.

1.6.6.3. Análise dos resultados e priorização das vulnerabilidades.

1.6.6.4. Elaboração e entrega de um Plano de Remediação considerando a criticidade da vulnerabilidade identificada e, também, os critérios definidos na fase de Levantamento de Ativos.

1.6.6.4.1. A remediação será feita pela CONTRATADA responsável pelo equipamento/solução, conforme a matriz de responsabilidades presente na tabela 4.2 do Termo de Referência.

1.6.6.5. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrever de forma detalhada as ações para correção. Caso precise ter acesso as configurações dos ativos de tecnologia ou o código fonte para propor as soluções de correção, a CONTRATADA deverá justificar a necessidade, ficando a cargo da CONTRATANTE decidir pela liberação.

1.6.6.6. Deve ser também apresentado a Matriz de Risco das vulnerabilidades detectadas e o grau de maturidade da CONTRATANTE em cada item analisado.

1.6.7. A solução de gerenciamento de vulnerabilidades de segurança (item 8 da Tabela 1.1 do TR) deve seguir os itens conforme abaixo:

1.6.7.1. O licenciamento da plataforma deverá ser pelos ativos descritos abaixo:

1.6.7.1.1. Ativos em rede.

1.6.7.1.2. Servidores e Estações de trabalho ou Notebooks.

1.6.7.1.3. Servidores em Cloud.

1.6.7.1.4. Contêineres. e

1.6.7.1.5. Aplicações Web e API.

1.6.7.2. A licença utilizada na prestação dos serviços deverá possibilitar a utilização dos ativos do item anterior.

1.6.7.3. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento.

1.6.7.4. O gerenciamento da solução deverá ser em nuvem.

1.6.7.5. O processo de análises de vulnerabilidades e conformidade, quando executados on-premises, deverá ser efetuado localmente, ou seja, na própria rede da CONTRATANTE ou com agente instalado no próprio computador. Os dados então serão sincronizados com a console em nuvem para análise.

1.6.7.6. A solução em nuvem deverá atender, no mínimo, os seguintes requerimentos de segurança:

1.6.7.6.1. A solução deve prover no mínimo 99% de disponibilidade no nível de serviço.

1.6.7.6.2. A solução deve criptografar todas as informações em trânsito.

1.6.7.6.3. Deve utilizar no mínimo chave AES-256 para criptografar os dados armazenados.

1.6.7.6.4. A solução deve ser capaz de gerar uma chave randômica para cada scanner conectado na plataforma de gerência.

1.6.7.6.5. Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados no mínimo com protocolo TLS 1.2 com tamanho de chave de 4096 bits.

1.6.7.6.6. Dados indexados devem possuir no mínimo criptografia utilizando algoritmo AES-256.

1.6.7.6.7. A plataforma deve utilizar no mínimo chave AES-256 para Backups e dados Replicados.

1.6.7.6.8. Todas as credenciais armazenadas na plataforma deverão ser criptografadas com algoritmo AES-256, no mínimo.

1.6.7.7. A solução deve possuir no mínimo as seguintes certificações de privacidade e segurança:

1.6.7.7.1. EU-U.S Privacy Shield Framework.

1.6.7.7.2. Cloud Security Alliance (CSA) STAR.

1.6.7.7.3. A solução deve possuir ferramentas e processos automatizados para monitorar uptime, comportamentos anômalos e performance da plataforma.

1.6.7.7.4. Deve possuir retenção na nuvem de no mínimo 12 meses dos resultados dos scans realizados no ambiente.

1.6.7.7.5. Os dados de clientes deverão ser totalmente separados um dos outros, não possuindo compartilhamento de dados.

1.6.7.7.6. O fabricante da solução deverá implementar controles de segurança, como Análise de Vulnerabilidade no mínimo semanal, Firewalls, segmentação de rede, e monitoramento de segurança 24/7/365, para garantir a segurança da aplicação.

1.6.7.7.7. O desenvolvimento da solução deverá seguir metodologias de Desenvolvimento Seguro.

1.6.7.7.8. A fabricante da solução deverá possuir ISO 27001.

1.6.7.7.9. Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo.

1.6.7.7.10. O gerenciamento da solução deve ser 100% em nuvem.

1.6.7.7.11. A solução deve prover no mínimo 99% de disponibilidade no nível de serviço.

1.6.7.7.12. A solução deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware).

1.6.7.7.13. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede.

1.6.7.8. Deve possibilitar, por meio da console, no mínimo 3 (três) métodos de escaneamento:

1.6.7.8.1. Scan ativo.

1.6.7.8.2. Scan passivo. e

1.6.7.8.3. Scanner em nuvem.

1.6.7.9. A solução deverá possuir Scanners em Nuvem em diversas localidades, possibilitando a escolha da localidade no momento do Scan. O uso destes scanners deverá estar contemplado no licenciamento.

1.6.7.10. Os Scanners em Nuvem devem estar disponíveis, no mínimo, em duas das seguintes localidades: EUA, Europa e Brasil.

1.6.7.11. Deve ser capaz de identificar vulnerabilidades, com seus respectivos CVEs, nas Imagens-Base de Contêineres. Além disso, deve ser capaz de identificar vulnerabilidades, portas abertas e os serviços em execução nos Contêineres (Imagens-Base em execução).

1.6.7.12. Deverá possuir, através de site público, uma lista com todas as vulnerabilidades identificadas pela solução.

1.6.7.13. A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferente do padrão CVSS.

1.6.7.14. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial (machine learning).

1.6.7.15. O Algoritmo de priorização deve considerar no mínimo 40.000 vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade.

1.6.7.16. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades.

1.6.7.17. A solução deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar mais de 20 fontes de dados relacionadas a vulnerabilidades.

1.6.7.18. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

1.6.7.18.1. CVSSv3 Impact Score.

1.6.7.18.2. Idade da Vulnerabilidade.

1.6.7.18.3. Se existe ameaça ou Exploit que explore a vulnerabilidade.

1.6.7.18.4. Número de produtos afetados pela vulnerabilidade.

1.6.7.18.5. Intensidade baseada no número e frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo.

1.6.7.18.6. Lista de todas as fontes (canais de mídia social, Dark Web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade.

1.6.7.19. A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação).

1.6.7.20. Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras.

1.6.7.21. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas como também de fontes não gratuitas.

1.6.7.22. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

1.6.7.23. A solução deve possuir conectores para a seguintes plataformas:

1.6.7.23.1. Amazon Web Service (AWS).

1.6.7.23.2. Microsoft Azure.

1.6.7.23.3. Google Cloud Platform.

1.6.7.23.4. Oracle Cloud.

1.6.7.24. A solução deve ser capaz de analisar vulnerabilidades em servidores na AWS utilizando somente o conector, sem a necessidade de instalação de agente ou uso de qualquer outro tipo de sensor de rede da solução.

1.6.7.25. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML.

1.6.7.26. A solução deve ser PCI ASV (Approved Scanning Vendor).

1.6.7.27. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan.

1.6.7.28. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.

1.6.7.29. A solução deve ser licenciada para no mínimo 50 scanners ativos.

1.6.7.30. A solução deve ser licenciada para o uso de no mínimo 20 sensores passivos de rede para realizar o monitoramento em tempo real do ambiente.

1.6.7.31. Deve ser possível determinar quais portas estão abertas em determinado ativo.

1.6.7.32. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:

1.6.7.32.1. Endereço IPv4 e IPv6.

1.6.7.32.2. Sistema Operacional.

1.6.7.32.3. Nome NetBIOS:

1.6.7.32.4. FQDN.

1.6.7.33. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

1.6.7.33.1. Bancos de dados.

1.6.7.33.2. Hypervisors.

1.6.7.33.3. Dispositivos móveis.

1.6.7.33.4. Dispositivos de rede.

1.6.7.33.5. Endpoints.

1.6.7.33.6. Aplicações.

1.6.7.34. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente.

1.6.7.35. Deve ter a capacidade de guardar em tempo real informações de GET e POST que trafeguem na rede.

1.6.7.36. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real.

1.6.7.37. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados.

1.6.7.38. A solução deve ser licenciada para uso de agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, para o número total de ativos contratados.

1.6.7.39. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors e Dispositivos de Rede.

1.6.7.40. -A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

1.6.7.41. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento de configurações e vulnerabilidades.

1.6.7.42. A solução deve incluir a capacidade de programar períodos em que varreduras não podem ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, etc), hora de início e fim da janela, quais ativos serão excluídos e o fuso horário do agendamento.

1.6.7.43. A solução deve ser configurável para permitir a otimização das configurações de varredura, permitindo no mínimo definir o período de timeout, o número de conexões TCP concorrentes e reduzir a análise em execução caso detecte congestionamento de rede.

1.6.7.44. Deve permitir executar uma análise de remediação, para verificar que uma solução foi aplicada corretamente. Essa análise de remediação será executada somente nos ativos impactados, analisando somente a vulnerabilidade remediada, sendo sua política criada especificamente para esta finalidade.

1.6.7.45. Deverá ser possível agrupar sensores em grupos

1.6.7.46. A solução deverá automaticamente distribuir uma atividade de análise entre os sensores pertencentes ao grupo, para aumentar a performance de um scan.

1.6.7.47. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é nova, persistente, corrigida ou reapareceu no ativo.

1.6.7.48. Deverá ser possível aceitar uma vulnerabilidade, de forma que não mais apareça na console. Este processo poderá ser feito para um único ativo ou múltiplos ativos. Ainda, deverá ser possível definir uma data de expiração para a Aceitação.

1.6.7.49. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos, podendo ainda definir uma data de expiração para esta modificação.

1.6.7.50. A solução deve suportar o uso de Tags nos ativos, sendo estes aplicados de forma manual ou automaticamente.

1.6.7.51. No caso de Tags, deverá ser possível configurar regras para atender, no mínimo:

1.6.7.51.1. Ativo analisado ou não em relação a vulnerabilidades.

1.6.7.51.2. Informações de nuvem pública, como por exemplo Região na AWS, Azure Resource ID ou GCP Cloud Project ID.

1.6.7.51.3. Software instalado no ativo.

1.6.7.51.4. Sub-rede.

1.6.7.51.5. Sistema Operacional.

1.6.7.52. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags.

1.6.7.53. A solução deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag.

1.6.7.54. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a Tag Linux.

1.6.7.55. A solução deve suportar RBAC (Role Based Access Control) com no mínimo 5 tipos de usuários pré-definidos.

1.6.7.56. Deve possuir no mínimo um perfil administrador e um perfil somente leitura.

1.6.7.57. Deve permitir autenticação com Single Sign On suportando os padrões SAML 2.0 ou Shibboleth 1.3.

1.6.7.58. A solução deve possibilitar a criação de Grupos de Usuários ou Grupos de Ativos gerenciados por um ou mais usuários.

1.6.7.59. Deve permitir configurar quais usuários, ou grupos de usuários, tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar análises de vulnerabilidades nesses ativos.

1.6.7.60. Possuir duplo fato de autenticação nativo na própria solução.

1.6.7.61. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades. No mínimo deverá ser possível configurar permissões de Nenhum Acesso, Somente Ver Resultados, Configuração ou Execução das políticas.

1.6.7.62. Deve ser capaz de exportar dashboards em modelo de relatórios, tanto de forma manual e periódico de acordo com a frequência estabelecida pelo administrador.

1.6.7.63. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável).

1.6.7.64. A solução deve suportar o envio automático de relatórios para destinatários específicos.

1.6.7.65. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual.

1.6.7.66. A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade.

1.6.7.67. Deve possuir ao menos 10 modelos de dashboards já criados, podendo ser customizados.

1.6.7.68. A solução deve permitir exportar dados do que está sendo apresentado na tela, no mínimo para:

1.6.7.68.1. Ativos gerenciados pela solução.

1.6.7.68.2. Todas as vulnerabilidades existentes nos ambientes e em quais ativos ela existe.

1.6.7.68.3. Vulnerabilidades por ativo gerenciado pela solução.

1.6.7.68.4. Vulnerabilidades de um único ativo.

1.6.7.68.5. Uma única vulnerabilidade e todos os ativos que possuem.

1.6.7.69. Deve ser possível exportar os dados em HTML, PDF ou CSV.

1.6.7.70. Em caso de exportação por CSV deve ser possível selecionar, via console de gerenciamento, quais campos deseja exportar.

1.6.7.71. Deve ser possível exportar somente os gráficos dos dashboards, através da console de gerenciamento, em PDF ou PNG ou JPG.

1.6.7.72. Deve ser possível criar um Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro Dashboard a aparecer na console no acesso.

1.6.7.73. Deve ser possível configurar um filtro permanente no Dashboards para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente.

1.6.7.74. A solução deve permitir compartilhar Dashboards com um ou mais usuários, bem como com grupo de usuários da aplicação.

1.6.7.75. Deve ser possível configurar SLAs em dias, representando a idade das vulnerabilidades no ambiente, sendo o período em que a mesma foi encontrada até a resolução. Está informação deverá ser apresentada no Dashboard da solução:

1.6.7.76. A solução deve ser totalmente licenciada para realizar scans de auditoria e compliance.

1.6.7.77. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino.

1.6.7.78. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada.

1.6.7.79. Toda a solução deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL.

1.6.7.80. A solução deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA ou MSCT (Microsoft Security Compliance Toolkit).

1.6.7.81. Deve suportar a verificação de compliance para no mínimo:

1.6.7.81.1. Cisco IOS.

1.6.7.81.2. Citrix Xenserver.

1.6.7.81.3. Check Point Firewall

1.6.7.81.4. Fortinet FortiOS.

1.6.7.81.5. Netapp Data ONTAP.

1.6.7.81.6. Palo Alto Firewall.

1.6.7.81.7. Red Hat Enterprise Virtualization.

1.6.7.81.8. Unix.

1.6.7.81.9. Windows.

1.6.7.81.10. VMware.

1.6.7.82. A solução deve mostrar se o critério de compliance foi atendido ou não fornecendo no mínimo os seguintes status: Passou, Falhou e Atenção.

1.6.7.83. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional.

1.6.7.84. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade.

1.6.7.85. Deve ser capaz de calcular a criticidade dos ativos da organização.

1.6.7.86. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE baseado nos processos desenvolvidos pelo CIS.

1.6.7.87. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização.

1.6.7.88. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

1.6.7.89. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

1.6.7.90. A solução deve permitir um acompanhamento histórico do nível de exposição da organização.

1.6.7.91. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

1.6.7.92. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade.

1.6.7.93. A solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução.

1.6.7.94. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área.

1.6.7.95. A solução deve permitir a segregação lógica entre aplicações distintas da empresa afim de obter a pontuação referente exposição cibernética por aplicação.

1.6.7.96. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados.

1.6.7.97. A solução deverá capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS).

1.6.7.98. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10).

1.6.7.99. Deve possui modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados.

1.6.7.100. Para varreduras extensas e detalhadas, deve varrer no mínimo os seguintes elementos:

1.6.7.100.1. Cookies, Headers, Formulários e Links.

1.6.7.100.2. Nomes e valores de parâmetros da aplicação.

1.6.7.100.3. Elementos JSON e XML.

1.6.7.100.4. Elementos DOM

1.6.7.101. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação.

1.6.7.102. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário.

1.6.7.103. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares.

1.6.7.104. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões.

1.6.7.105. Deve ser capaz de configurar parâmetros para controle de performance ou de limitar os itens a seguir:

1.6.7.105.1. URLs para crawl e navegação.

1.6.7.105.2. Diretórios para varreduras.

1.6.7.105.3. Profundidade dos elementos DOM.

1.6.7.105.4. Máximo de respostas.

1.6.7.105.5. Requisições de redirecionamentos.

1.6.7.105.6. Tempo para a varredura.

1.6.7.105.7. Número de conexões HTTP ao servidor hospedando a aplicação Web.

1.6.7.105.8. Número de requisições HTTP por segundo.

1.6.7.106. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual.

1.6.7.107. Deve ser capaz de enviar notificações através de no mínimo E-mail.

1.6.7.108. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques.

1.6.7.109. Deverá avaliar sistemas web utilizando frameworks modermos, como AJAX, HTML5 e SPA.

1.6.7.110. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes.

1.6.7.111. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger).

1.6.7.112. Deverá suportar no mínimo os seguintes esquemas de autenticação:

1.6.7.112.1. Autenticação básica (digest).

1.6.7.112.2. NTLM.

1.6.7.112.3. Form de login.

1.6.7.112.4. Autenticação de Cookies.

1.6.7.112.5. Autenticação através de Selenium.

1.6.7.113. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário.

1.6.7.114. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos.

1.6.7.115. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise.

1.6.7.116. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

1.6.7.117. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações.

1.6.7.118. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes.

1.6.7.119. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

1.6.7.119.1. Payload injetado.

1.6.7.119.2. Evidência em forma de resposta da aplicação.

1.6.7.119.3. Detalhes da requisição HTTP.

1.6.7.119.4. Detalhes da resposta HTTP.

1.6.7.120. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas.

1.6.7.121. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas.

1.6.7.122. A solução deve possuir suporte a varreduras de componentes para no mínimo: sistemas de gerenciamento de conteúdo (CMS), frameworks de desenvolvimento web, servidores web e de aplicação, bibliotecas JavaScript, plataformas de e-commerce, bibliotecas AJAX e frameworks de interface de usuário, além de outras ferramentas amplamente utilizadas no desenvolvimento e operação de aplicações web e sistemas empresariais.A solução deverá possuir controle de permissão de usuários, com no mínimo menos 3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura.

1.6.7.123. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução.

1.6.7.124. A solução deverá possuir um Add-on para o browser que permite gravar uma macro de autenticação para criação do Selenium.

1.6.7.125. A solução deverá possuir nativamente scanners pré-configurados em nuvem, para realização de scans externos. Estes scanners deverão obrigatoriamente possuir IP dedicado, com divulgação pública, para configuração de whitelist em Firewalls, WAFs, ou outros sistemas de proteção.

1.6.7.126. A solução deve possuir também sensores (scanner) on-premises. A solução deverá estar licenciada para o uso de no mínimo 10 sensores deste tipo.

1.6.7.127. Deverá ser possível exportar os gráficos do dashboard em PDF ou PNG ou JPEG, nativamente pela console de gerência.

1.6.7.128. A solução deve suportar listas de exclusão globais.

1.6.7.129. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas.

1.6.7.130. Ser possível gerar relatório das vulnerabilidades, no mínimo em PDF, HTML e CSV.

1.6.7.131. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem.

1.6.7.132. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados.

1.6.7.133. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos.

1.6.7.134. A solução deve ser capaz de se integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual da CONTRATANTE.

1.6.7.135. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante.

1.6.7.136. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens.

1.6.7.137. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas.

1.6.7.138. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção.

1.6.7.139. A solução deve analisar as camadas (layers) de um container.

1.6.7.140. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção.

1.6.7.141. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas.

1.6.7.142. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem.

1.6.7.143. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual.

1.6.7.144. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem.

1.6.7.145. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

1.6.7.145.1. Docker.

1.6.7.145.2. AWS ECR.

1.6.7.145.3. JFrog Artifactory.

1.6.7.146. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE.

1.6.7.147. A solução ser capaz de configurar políticas usando como condições as vulnerabilidades mapeadas pela solução, incluindo o nivel de severidade de cada uma delas.

1.6.7.148. Caso a condição da política seja verdadeira, a solução deve ser capaz de prevenir o pull destas para implementação ou identificar a falha de compliance das imagens para ação do time de segurança.

1.6.7.149. A solução deve permitir a criação de políticas especificas por repositório.

1.6.7.150. A solução deve prover integração com plataformas de integração contínua amplamente utilizadas no mercado, permitindo compatibilidade com ferramentas que suportem automação de pipelines de CI/CD, orquestração de contêineres e outras tecnologias relacionadas.

1.6.7.151. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser:

1.6.7.151.1. Nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a container, algumas já explicitadas em itens anteriores, e já licenciada para uso.

1.6.7.151.2. Executada através de integração com terceiros, desde que toda a solução esteja licenciada para a CONTRATANTE.

1.6.7.152. Será de responsabilidade da CONTRATADA prover a solução para gestão de vulnerabilidades para todo o escopo deste documento, bem como operar, sustentar, suportar e apresentar a melhoria contínua da ferramenta durante todo o período de vigência do contrato.

1.6.7.153. A solução para gestão de vulnerabilidades deverá estar licenciada para, no mínimo, 1500 dispositivos ou IPs, sendo:

DESCRIÇÃO	QTD.
Servidores físicos e virtuais	700
Ativos de rede e segurança (onprimisse e cloud)	120
Aplicações web	150
Estações de trabalho (por amostragem)	400
Containers	80
Telefones VoIP, câmeras IP, impressoras etc	50
TOTAL	1500

1.6.7.154. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, os seguintes indicadores chave de desempenho vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal segurança da CONTRATADA, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades internas e na nuvem	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades críticas por área responsável	Soma de vulnerabilidades críticas por área responsável	Vulnerabilidades críticas	Vulnerabilidades	Número total de vulnerabilidades críticas por área responsável
Quantitativo de vulnerabilidades corrigidas	Soma de vulnerabilidades corrigidas	Vulnerabilidades corrigidas	Vulnerabilidades	Número total de vulnerabilidades corrigidas

Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB	Soma de vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades corrigidas em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB
Quantitativo de vulnerabilidades em ativos	Soma de vulnerabilidades em ativos	Vulnerabilidades em ativos	Vulnerabilidades	Número total de vulnerabilidades em ativos
Quantitativo de vulnerabilidades corrigidas em ativos	Soma de vulnerabilidades corrigidas em ativos	Vulnerabilidades corrigidas em ativos	Vulnerabilidades	Número total de vulnerabilidades corrigidas em ativos
Quantidade de vulnerabilidades em códigos de aplicações	Soma de vulnerabilidades em códigos de aplicações	Vulnerabilidades em códigos de aplicações	Vulnerabilidades	Número total de vulnerabilidades em códigos de aplicações
Patches aplicados em dia	Percentual dos patches críticos aplicados dentro da janela	Vulnerabilidades críticas	Vulnerabilidades	Percentual dos patches críticos aplicados dentro da janela
Patches aplicados em dia por ativo	Percentual dos patches críticos aplicados dentro da janela para cada tipo de ativo	Ativos: serv Linux, serv Win, estações, dispmóveis, etc.	Vulnerabilidades	Percentual dos patches críticos aplicados dentro da janela para cada tipo de ativo
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados

1.6.7.155. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Certified Incident Handler), GMON (GIAC Continuous Monitoring) ou profissional com comprovada experiência no tratamento de incidentes de segurança de grande impacto técnico e institucional. Nesse contexto, esse profissional deve apresentá-lo de forma presencial nas dependências da CONTRATADA em Brasília/DF ou de forma virtual, por meio de solução de videoconferência.

1.7. SEGURANÇA DE REDES

1.7.1. Tem por objetivo a monitoração, sustentação, operação e evolução das ferramentas e tecnologias de segurança da informação em uso pela ANAC (firewalls, IDS, IPS, WAF e etc), descritas no Anexo II - Ambiente Tecnológico, com suporte de atendimento remoto e, para os casos que o exigirem, atendimento presencial.

1.7.2. Este serviço ainda tem por finalidade e responsabilidade, gerenciar todo o ciclo de vida de todas dos serviços, referente ao parque de segurança da informação da CONTRATANTE, visando:

1.7.2.1. Oferecer canais de comunicação integrados para funcionários autorizados do corpo técnico da CONTRATANTE requisitarem e receberem devolutivas de serviços pré-definidos, presentes no catálogo de serviço do presente instrumento.

1.7.2.2. Realizar mudanças padrões, pré-definidas e presente no catálogo de serviço do presente instrumento.

1.7.2.3. Desenvolver atividades proativas para manutenção, continuidade e evolução da infraestrutura e serviços de segurança da informação da CONTRATADA sob sua responsabilidade.

1.7.2.4. Propor, documentar, implantar, verificar e aprimorar processos e procedimentos operacionais que garantam a eficiência, eficácia e efetividade dos serviços de segurança da informação sob sua responsabilidade.

1.7.2.5. Realizar o levantamento e documentar dos serviços de segurança da informação existentes no ambiente da CONTRATADA, bem como propor e implantar novos serviços.

1.7.2.6. Realizar a monitoração dos níveis de serviço entregues, de acordo com parâmetros e indicadores estabelecidos na presente contratação.

1.7.2.7. Atuar na identificação, registro e tratamento de incidentes que afetem os serviços de TIC da CONTRATADA sob sua responsabilidade.

1.7.2.8. Acompanhamento do nível de satisfação dos usuários sobre os serviços de TIC da CONTRATADA sob sua responsabilidade.

1.7.2.9. Participar de reuniões de alinhamento de tarefas com demais equipes de desenvolvimento e infraestrutura.

1.7.2.10. Apoiar na definição tecnológica e escolha de soluções de TIC.

1.7.2.11. Propor a configuração de itens de monitoração.

1.7.2.12. Documentar e realizar a transferência de conhecimento às equipes da ANAC sempre que requisitado.

1.7.2.13. Definir e manter convenções de nomenclatura a ser utilizado para os ativos de TIC, conforme aprovação da ANAC.

1.7.2.14. Acionar e acompanhar o atendimento do suporte técnico do fabricante ou do fornecedor do ativo de segurança nas situações necessárias.

1.7.3. Os serviços de operação deverão atuar e apoiar no processo de tratamento de incidentes em regime de plantão 24x7x365, que venham a ser reportados no escopo de serviço de outros contratos da ANAC, sem custo adicional.

1.7.4. Para a execução das atividades, será definido um catálogo de serviço pré-estabelecido pela CONTRATANTE, não se limitando apenas a este, em que se espera que a CONTRATADA defina e realize de forma periódica ações proativas para melhoria das ferramentas sob sua responsabilidade.

1.7.5. O serviço deverá ser prestado tendo por base as melhores práticas de mercado difundidas pela ITIL, COBIT, ISO/IEC 20.000 e a série de normas ISO/IEC 27.000.

1.7.6. As atividades de cabeamento estruturado, referentes à conexão dos equipamentos e soluções de segurança aos ativos de redes da ANAC ficarão a cargo do atual contrato de Service Desk, estando, portanto, fora do escopo desse serviço.

1.7.7. Solicitantes Autorizados e Qualidade dos Atendimentos

1.7.8. Uma das origens de requisição de serviço poderá ser via interface humana, e a fim de evitar possíveis alterações anômalas e indesejadas no ambiente de segurança da informação, apenas funcionários autorizados do corpo técnico da CONTRATANTE, poderão realizar abertura de requisições de serviços.

1.7.9. Sempre que uma nova requisição de serviço for solicitada, pelo corpo técnico da CONTRATANTE, a CONTRATADA deverá previamente observar se tal contato está autorizado a solicitar tais serviços, antes de iniciar o atendimento. Caso tal contato não seja autorizado, o atendimento não deverá ser iniciado, e um comunicado de tentativa de abertura de atendimento não autorizado, deve ser enviado ao gestor de contrato por parte da CONTRATANTE.

1.7.10. A CONTRATADA deverá manter uma plataforma para gerir tais contatos autorizados, constando ao menos as seguintes informações dos contatos: nome, telefone, e-mail, cargo. O gerenciamento (criar, atualizar, desativar e remover) desta plataforma deve estar disponível via internet para a CONTRATANTE, seguindo os critérios de segurança estabelecido para o sistema de ITSM, ou seja, acessível via internet utilizando protocolo TLS 1.2 ou superior, com certificado digital emitido em nome da CONTRATADA.

1.7.11. A plataforma de gestão de contatos autorizados deve ter a capacidade de relacionar os contatos autorizados com os itens de configuração de sua responsabilidade do ambiente de segurança da informação da CONTRATANTE.

1.7.12. Nos primeiros 30 (trinta) dias iniciais do contrato, a CONTRATANTE informará através de e-mail destinado a CONTRATADA, sobre quem e quantos são os contatos autorizados, bem como uma matriz de responsabilidade relacionado aos itens de configuração que compõem a arquitetura de segurança da informação da CONTRATANTE.

1.7.13. Após o recebimento da notificação a CONTRATADA deverá, em até 15 (quinze) dias, disponibilizar os acessos aos canais de comunicação, a todos os contatos autorizados. A CONTRATADA ainda deve enviar o comunicado de boas-vindas para cada contato, com manual de acesso a cada canal de comunicação, bem como também suas devidas credenciais.

1.7.14. O acesso aos canais de comunicação relacionado no presente termo, de qualquer tipo (telefonia, sistemas, e-mails) devem estar disponíveis para todos os contatos autorizados, a serem relacionados pela CONTRATANTE, independentemente da quantidade, exceto a sala virtual de crise, limitando-se a 10 (dez) pessoas simultaneamente por parte da CONTRATANTE.

1.7.15. No fechamento de toda e qualquer requisição de serviço, independente da severidade e/ou tempo de atendimento, a CONTRATADA deverá enviar uma pesquisa de satisfação para o solicitante. Tal pesquisa deve se basear no método NPS do inglês Net Promoter Score.

1.7.16. Caso a satisfação do atendimento avaliado for menor do que 70% (setenta por cento), um analista de qualidade da CONTRATADA deverá entrar em contato com o requisitante do serviço, a fim de avaliar com mais detalhes e propriedade as razões pelas quais o atendimento não alcançou a satisfação desejada.

1.7.17. Posteriormente um processo de não conformidade deve ser aberto, e em até 7 (sete) dias uteis, deve ser apresentado à CONTRATANTE, um plano de ação de melhorias para que eventual insatisfação não volte a acontecer.

1.7.18. Grupo Técnico de Operações

1.7.18.1. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para resolver as requisições de serviço presencial no ambiente da CONTRATANTE, baseado nas tecnologias e fabricantes que compõe o parque de segurança da CONTRATANTE atualmente, a CONTRATADA obrigatoriamente deverá compor as tecnologias e produtos listados no ANEXO II, com ao menos 1 (um) perfil de cada que segue descrito abaixo:

1.7.18.2. Analista de segurança de redes:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Experiência comprovada de no mínimo 3 (três) anos em atividades relacionadas aos mecanismos de segurança e tratamentos de incidentes de segurança de TI, com conhecimento em tecnologias de firewall, IDS/IPS, SIEM, endpoint security (CheckPoint Sandblast ou similar), Anti-DDoS, Ethernet 802.1x, Radius, IPSEC VPN – Virtual Private Network (client-to-site e site-to-site).
Treinamentos/ Certificações	• ITIL v3 Fundation, ou superior • Certificação Check Point Certified Security Expert (CCSE) ou superior ou treinamento equivalente da ferramenta. • Certified Information Systems Auditor (CISA) ou CompTIA Security+ ou GIAC Security Essentials Certification (GSEC) ou GIAC Certified Incident Handler (GCIH) ou Offensive Security Certified Professional (OSCP) ou equivalente/superior. • Certified Information Security Manager (CISM) ou Systems Security Certified Practitioner (SSCP) ou equivalente/superior.

1.7.18.3. Analista de segurança de aplicação:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Experiência comprovada de no mínimo 3 (três) anos em atividades relacionadas a implantação, configuração e administração de solução de WAF (Web Application Firewall).
Treinamentos/ Certificações	• ITIL v3 Fundation, ou superior • Certified Information Systems Auditor (CISA) ou CompTIA Security+ ou GIAC Security Essentials Certification (GSEC) ou GIAC Certified Incident

	Handler (GCIH) ou Offensive Security Certified Professional (OSCP) ou equivalente/superior. • Certificação F5 Certified Technical Specialist BIG-IP Application Security Manager (ASM).

1.7.19. Na data de abertura da Ordem de Serviço será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do Grupo Técnico, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, curriculum vitae para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento.

1.7.20. Entregas a serem realizadas

1.7.21. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, deverão ser entregues os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de requisições abertas	Soma de requisições abertas	Requisições abertas	Requisições	Número total de requisições abertas
Quantitativo de requisições por função	Soma de requisições abertas por função	Requisições por função	Requisições por função	Número total de requisições por função
Quantitativo de requisições concluídas	Soma de requisições concluídas	Requisições concluídas	Requisições concluídas	Número total de requisições concluídas
Quantitativo de requisições em backlog	Soma de requisições em backlog	Requisições em backlog	Requisições em backlog	Número total de requisições em backlog
TOP 10 – Ativos configurados	Soma do número de configurações por ativo	Requisições por ativo	ativo	TOP do número de requisições por ativo
TOP 10 – Requisições por origem	Soma do número de requisições por origem	Requisições por origem	Origem	TOP do número de requisições por origem
TOP 10 – Aplicações configuradas	Soma do número de aplicações configuradas	Requisições por Aplicações	Aplicações	TOP 10 requisições por aplicações

1.7.22. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC

Incident Handler) ou GMON (GIAC Continuous Monitoring. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da CONTRATANTE ou de forma virtual, por meio de solução de videoconferência.

1.8. SEGURANÇA DE APLICAÇÃO

1.8.1. A execução desse serviço tem como objetivo o atendimento dos controles e medidas de segurança presentes no framework do Programa de Privacidade e Segurança da Informação – PPSI/SGD:

1.8.1.1. **Controle 16 – segurança de aplicações:** Gerenciar o ciclo de vida da segurança de software desenvolvido, hospedado ou adquirido internamente para prevenir, detectar e corrigir os pontos fracos de segurança antes que possam afetar a ANAC.

1.8.2. Atividades a serem executadas pela CONTRATADA:

1.8.2.1. Apoiar o estabelecimento e manutenção de um processo seguro de desenvolvimento de aplicações, tratando itens como padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação. A documentação deve ser atualizada e revisada anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.

1.8.2.2. Apoiar o estabelecimento e manutenção de um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações que facilite a priorização da ordem em que as vulnerabilidades descobertas são corrigidas. Esse processo inclui a definição de um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. As classificações de gravidade trazem uma forma sistemática de triagem de vulnerabilidades que melhora a gestão de riscos e ajuda a garantir que os bugs mais graves sejam corrigidos primeiro. O sistema e o processo devem ser revisados e atualizados anualmente.

1.8.2.3. Definir modelos de configuração de segurança padrão recomendados pelo setor para componentes de infraestrutura de aplicações. Isso inclui servidores subjacentes, bancos de dados e servidores web e se aplica a contêineres de nuvem, componentes de Platform as a Service (PaaS) e componentes de SaaS.

1.8.2.4. Implementar verificações de segurança em nível de código, aplicando ferramentas de análise estáticas e dinâmicas dentro do ciclo de vida da aplicação para verificar se as práticas de codificação seguras estão sendo seguidas.

1.8.3. Ferramentas

1.8.3.1. Para a execução dos serviços de segurança de aplicação, a CONTRATADA poderá utilizar as soluções e ferramentas já em uso pela ANAC. Caso identifique a necessidade de ferramentas adicionais, as mesmas poderão ser fornecidas pela CONTRATADA, sem custos adicionais à CONTRATANTE, sendo permitido o uso de soluções open source. A relação de ferramentas em uso pela Anac está listada no Anexo II - Ambiente Tecnológico.

1.8.3.1.1. No caso de adoção de ferramentas open source, a instalação deverá ser feita em ambiente computacional disponibilizado pela CONTRATANTE, podendo ser on-premise ou em cloud, e ao final do

contrato, a ferramenta instalada será mantida no ambiente da ANAC, inclusive com seus dados.

1.8.3.1.2. No caso de adoção de ferramentas comerciais que não sejam de propriedade da ANAC, a instalação poderá ser feita no ambiente computacional da ANAC ou da CONTRATADA, e ao final do contrato, os dados brutos deverão ser disponibilizados para a ANAC, em formato XML, JSON, CSV, ou outro que venha a ser aceito pela CONTRATANTE.

1.8.4. A contratada deverá atuar no estabelecimento e execução de processos relacionados aos respectivos controles, bem como no apoio e orientação quanto às ações necessárias para o aumento da maturidade da ANAC junto a demais contratos, de acordo com as medidas de segurança de cada um dos controles.

1.8.5. A CONTRATADA deverá revisar as políticas e os processos relacionados aos temas já existentes na ANAC e, na sua ausência, deverá providenciá-los, em até 90 (noventa) dias do início da execução dos serviços. A CONTRATADA irá propor um cronograma de entrega dos processos, revisados ou escritos, para acompanhamento da equipe de fiscalização do contrato.

1.8.6. Perfil profissional:

Formação	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação OU de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC).
Experiência	Possuir no mínimo 03 anos na área de segurança da informação.
Treinamentos/ Certificações	Possuir ao menos 1 (uma) das certificações abaixo: • CompTIA Security+ ou equivalente. • CCNA Security+ ou equivalente. • CEH Certified Ethical Hacker ou OSCP Offensive Security Certified Professional. • Check Point Certified Security Administrator (CCSA) ou equivalente. • Certificação em administração de solução de em Endpoint ou EDR. • F5 BIG-IP Certified Administrator, F5 BIG-IP ASM Certified Technical Specialist ou F5 BIG-IP LTM Certified Technical Specialist. • Certificação em administração de solução DDoS. • Microsoft 365 Certified: Security Administrator Associate, Microsoft Certified. • Associate ou Microsoft Certified: Security, Compliance, and Identity Fundamentals.

	• EXIN Information Security Management Professional based on ISO/IEC 27001. • ISO 27001:2013 Auditor Interno. • ISO 27001:2022 Auditor Líder. • ISO 27001:2022 Lead Implementer.

1.8.7. Entregas a Serem Realizadas

1.8.7.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a CONTRATANTE definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Procedimentos de Teste de Segurança	Percentual de aplicações que passaram por testes de segurança antes da liberação	Teste de Segurança	Segurança de aplicação	Apoiar o estabelecimento e manutenção de um processo seguro de desenvolvimento de aplicações
Segurança de Código de Terceiros	Percentual de código de terceiros revisado e aprovado para segurança.	Código de Terceiros	Segurança de aplicação	Apoiar o estabelecimento e manutenção de um processo seguro de desenvolvimento de aplicações
Conformidade com Modelos de Configuração	Percentual de componentes de infraestrutura configurados de acordo com os modelos de segurança padrão.	Modelos de Configuração	Segurança de aplicação	Validar se componentes de infraestrutura de aplicações estão acordo com modelos de configuração de segurança padrão.
Cobertura de Análise Estática e Dinâmica	Percentual de código analisado por ferramentas de análise estática e dinâmica.	Análise SAST e DAST	Segurança de aplicação	Implementar verificações de segurança em nível de código, aplicando ferramentas de análise estáticas e dinâmicas

2. **ESPECIFICAÇÃO DOS SERVIÇOS DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS - LOTE 02**

2.1. O serviço de Inteligência de Ameaças Cibernéticas (do inglês, Cyber Threat Intelligence - CTI) deve ser implantado no ambiente tecnológico da CONTRATADA, portanto, em ambiente externo à ANAC, podendo ser considerado um serviço do tipo Software as a Service

2.2. O serviço de CTI irá gerar eventos que terão como produtos a detecção de citações, termos ou referências aos ativos de informação e de TIC monitorados, seja na deep/dark web, na internet aberta, em páginas de compartilhamento, redes sociais e aplicativos monitorados. Esses Eventos serão gerados pela solução de inteligência de ameaças cibernéticas utilizada pela CONTRATADA para execução deste serviço. A relação de ativos monitorados será fornecida pela ANAC, cabendo à CONTRATADA a responsabilidade por avaliar se todos os insumos para a correta geração dos eventos estão sendo repassados corretamente para a ferramenta de CTI.

2.3. Caso a CONTRATADA identifique a ausência de insumos necessários para a geração dos Eventos, será reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo. A ANAC, sempre que solicitada, repassará para a CONTRATADA as informações necessárias para aprimorar este processo.

2.4. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. A CONTRATANTE fará processo de revisão e pode determinar a alteração de categorias dos eventos de CTI.

2.5. O serviço deverá ser acessível, através de API e Console, por meio de login e senha, com as seguintes características:

2.5.1. Devem ser disponibilizados no mínimo de 7 (sete) usuários com acessos simultâneos.

2.5.2. Um dos acessos simultâneos deve ser disponibilizado via API, preferencialmente API REST, para integração aos demais processos do SOC.

2.5.3. Deve ser capaz de receber chamadas REST API via serviço web utilizando o protocolo HTTPS com TLS 1.2 com autenticação no mínimo: chave, senha e certificado.

2.5.4. A ANAC poderá solicitar a alteração de login e senha do acesso conforme a sua necessidade.

2.5.5. O serviço não deve ser instalado na infraestrutura de TIC da ANAC.

2.5.6. A autenticação para acesso ao sistema deverá contar com duplo fator de autenticação (2FA), oferecendo, no mínimo, uma das opções: E-mail ou One Time Password (OTP)

2.5.7. A opção de duplo fator de autenticação por meio de SMS deverá ser completamente implementada pela CONTRATADA, e o efetivo envio de mensagens deve ocorrer sem qualquer custo adicional para a ANAC

2.6. Da Confidencialidade, Integridade e Disponibilidade dos dados de CTI, a CONTRATADA deverá:

2.6.1. Implementar os controles necessários para que apenas os seus profissionais, bem como os usuários e grupos criados por esta instituição, tenham acesso às pesquisas realizadas e aos dados armazenados.

2.6.2. Se responsabilizar pela guarda das informações coletadas por período a ser definido pela ANAC, não menor que 6 meses.

2.6.3. Realizar cópia de segurança dos dados coletados em razão dos ativos de informação monitorados, de forma a permitir ao menos a restauração das pesquisas realizadas e de seus resultados.

2.6.3.1. Essas informações, quando solicitadas pela ANAC, devem ser repassadas em pelo menos um dos seguintes nos formatos: JSON, HTML, PDF, CSV, Planilha eletrônica DOCX, ou em outros formatos aderentes ao E-Ping

2.6.4. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte.

2.6.5. Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todas as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, usuário, e ação/pesquisa efetuada

2.7. A Console de CTI deve:

2.7.1. Não limitar quantidade de recursos pesquisados.

2.7.2. Prover pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas.
2.7.3. Possibilitar que se monitore ameaças emergentes e se avalie a aplicabilidade, especificamente no ambiente da ANAC, com o objetivo de prevenir a exploração de alguma vulnerabilidade de segurança
2.7.4. Possuir modelos de filtro de informações pré-configurados na utilização das diferentes fontes de informação monitoradas
2.7.5. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.
2.7.6. Prover um campo de descrição em que os analistas de segurança cibernética da ANAC, ou da CONTRATADA, possam contextualizar as informações associadas aos eventos. Este recurso deve facilitar o consumo das informações de CTI pelas equipes de segurança cibernética, a exemplo das equipes do serviço de CSOC.
2.7.7. Apresentar a descoberta de páginas web de “phishing”, utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos de informação que serão protegidas.
2.7.8. Apresentar a verificação de sites suspeitos de phishing para domínios solicitados pela CONTRATANTE, ou que tenham sido levantados pela CONTRATADA. Para essa verificação deve-se utilizar, entre outras, as seguintes entidades reguladoras: ICANN (Internet Corporation for Assigned Names and Numbers) e Registro.Br (Registro de Domínios para a Internet do Brasil).
2.7.9. Apresentar a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa contra a ANAC como, por exemplo:
    2.7.9.1. Variações comuns de nomes.
    2.7.9.2. Permutações de caracteres. e
    2.7.9.3. Desvio de URL (typosquatting)
2.7.10. Os resultados das pesquisas no Console de CTI devem, no mínimo:
    2.7.10.1. Retornar os seguintes campos: contexto pesquisado, data, idioma, endereço web/deep web/dark web, conteúdo original completo.
    2.7.10.2. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo ordenáveis por data e hora da ocorrência mais recente para a mais antiga, e por tema, ameaça, entre outros.
    2.7.10.3. Permitir a atualização automática do resultado de pesquisas anteriormente realizadas com alertas visuais dessas atualizações.
    2.7.10.4. Disponibilizar os casos reportados para ANAC através de dashboard de gerenciamento de tickets, que permita a filtragem dos mesmos por, no mínimo: intervalo de data, contexto, status (aberto, em andamento, encerrado).
    2.7.10.5. Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada categoria de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web).
    2.7.10.6. Disponibilizar uma tela com informações consolidadas para visualização dos alertas cadastrados.
    2.7.10.7. Permitir exportar qualquer resultado de forma manual ou automática para, no mínimo, dois dos seguintes formatos: JSON, HTML, PDF, CSV, Planilha eletrônica, DOCX, ou em outros formatos aderentes ao E-Ping..
2.7.11. Este Serviço de INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS deve:
    2.7.11.1. Monitorar ameaças contidas na internet aberta, deep web e dark web, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da ANAC, do ponto de vista da segurança cibernética. O monitoramento nestes 3 ambientes compreende, mas não se limita, às mídias como: domínios, sites, blogs, vlogs, fóruns e IRCs.
    2.7.11.2. Monitorar as lojas de aplicativos Apple Store e Google Play com o objetivo de detectar aplicativos maliciosos que estejam relacionados com a ANAC. É de responsabilidade da CONTRATADA providenciar a remoção de aplicações falsas e maliciosas através de parcerias com as lojas de aplicativos, quando solicitadas pela ANAC.

2.7.11.3. Monitorar fontes de informações como Shodan, BinaryEdge, Zone-H, Bases de CVE, entre outras, bem como sites que compartilhem informações sobre TTPs utilizados para ataques como phishing, ransomware, entre outros.

2.7.11.4. Monitorar ameaças cibernéticas de forma direta ou indireta contidas nas fontes em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da ANAC, do ponto de vista da segurança cibernética. As fontes compreendem, mas não se limitam à: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Ghostbin, Scribd, Reclame Aqui, Apple Store, 4Shared, Google Play, Vimeo e Github, Gitlab e feeds RSS.

2.7.11.4.1. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, metadados e tipo da fonte.

2.7.11.5. Monitorar ameaças representadas por domínios suspeitos ou fraudulentos e em seguida realizar o takedown desses domínios. A CONTRATADA se obriga a realizar todo o processo para retirada do ar desses sites que contenham phishing ou sites que disparem spam utilizando-se do nome, da marca ou da imagem da ANAC, mesmo que similar, (com intuito de confundir e aplicar fraudes ou golpes nos usuários dos serviços prestados pela ANAC)

2.7.11.6. A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo Top-Level Domain (TLDs) e Generic Top-Level Domain (gTLDs) e Country Code Top-Level Domain (ccTLD), que verifique a utilização do uso indevido das marcas da ANAC no nome do domínio ou na URL, a empresa que administra o registro do domínio, e os dados do proprietário do domínio. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento do atendimento, para acompanhamento do processo de takedown de cada ocorrência

2.7.11.6.1. Fruto do monitoramento do item 2.7.11.4, pode ser necessário remover perfis falsos, desde que estejam relacionados com os ativos de informação monitorados. Será obrigação da CONTRATADA estabelecer parcerias com as principais redes sociais para os procedimentos de desativação desses perfis falsos, quando solicitado pela ANAC.

2.7.11.7. Monitorar ameaças, ataques e vulnerabilidades contidas em aplicativos de mensagens, como por exemplo WhatsApp e Telegram, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC da ANAC, do ponto de vista da segurança cibernética.

2.7.11.8. Monitorar os itens especificados de 2.7.11.1 a 2.7.11.5 em relação às ameaças cibernéticas, proteção de marcas ou tentativas de fraudes envolvendo produtos ou serviços que constarão em listagem fornecida pela ANAC após a assinatura do contrato. Esta listagem pode ser alterada a qualquer tempo pela CONTRATANTE.

2.7.11.9. Na Fase de Encerramento do Contrato (Transição Contratual) a CONTRATADA se obriga a fornecer backup das informações que foram geradas para os Eventos de Exceção ao longo de toda a execução contratual, em formato como JSON, HTML, PDF, CSV, Planilha eletrônica e DOCX, ou em outros formatos aderentes ao E-Ping, com o intuito de que se possa reutilizar essa base histórica de informações, inclusive em eventual nova contratação

2.7.11.10. Achados que devem ser reportados:

2.7.11.10.1. Sites utilizados para realizar, ou tentar realizar, golpes e fraudes que envolvam ou remetam de qualquer forma aos ativos de informação monitorados.

2.7.11.10.2. Anomalias nos registros “WhoIS” dos domínios monitorados.

2.7.11.10.3. Serviços que devem ser somente de consumo interno, sistemas e páginas internas (intranet) relacionados ao CONTRATANTE e que estejam expostas na internet, podendo ou não ser exploradas para eventuais ataques cibernéticos.

2.7.11.10.4. Vulnerabilidades dos domínios monitorados que foram tornadas públicas, mesmo que essa exposição esteja disponível apenas na deep e dark web.

2.7.11.10.5. Novas vulnerabilidades que tenham sido recentemente divulgadas para as tecnologias descritas no Anexo II - Ambiente Tecnológico.

2.7.11.10.6. Identificação de possíveis intenções de ataques a sistemas, serviços, ativos de informação e pessoas de interesse da ANAC que serão fornecidas a CONTRATADA na fase de Inserção da CONTRATADA.

2.7.11.10.7. Intenções de ataque que tenham como objetivo os ativos monitorados.

2.7.11.10.8. Campanhas relevantes de “hacktivismo”, como por exemplos ataques crescentes cujos alvos são em sua maioria órgão públicos ou de governo, ou ainda campanhas de ataques em que a vulnerabilidade explorada possa estar presente nas tecnologias implantadas na ANAC.

2.7.11.10.9. Comercialização online de informações sensíveis, informações pessoais, entre outras, das pessoas de interesse ou vinculadas à ANAC.

2.7.11.10.10. Atividades fraudulentas relacionadas aos ativos monitorados (utilização indevida de nome e marca, por exemplo).

2.7.11.10.11. Domínios ou IPs monitorados em listas de spam.

2.7.11.10.12. Credenciais de acesso aos ativos e Nuvem privada da ANAC que estejam, ou não, à venda na web aberta, dark web e deep web.

2.7.11.10.13. Credencias de correio eletrônico dos domínios monitorados que estejam, ou não, à venda na web aberta, dark web e deep web.

2.7.11.10.14. Códigos maliciosos (malwares) direcionados para os ativos e sistemas de informação monitorados.

2.7.11.10.15. Intenções diretas de ataques aos ativos e sistemas de informação monitorados.

2.7.11.10.16. Discussões online maliciosas que divulguem ou acompanhem informações dos ativos de informação monitorados.

2.7.11.10.17. Perfis falsos que utilizem os nomes e/ou fotos das pessoas de interesse da ANAC.

2.7.11.10.18. Documentos ou informações confidenciais, sensíveis ou sigilosas vazadas dos ativos de informação monitorados.

2.7.11.10.19. Aplicações (dispositivos móveis, softwares e aplicações web) falsas que utilizem o nome, a marca ou identidade visual dos ativos de informação monitorados.

2.7.11.10.20. Desfiguração de páginas (defacement) hospedadas nos domínios monitorados.

2.7.11.11. Reportar os achados dos monitoramentos previstos nos itens de 2.7.11.1 a 2.7.11.6 de quatro (4) formas:

a) por meio de e-mail e ligação telefônica em tempo real, se a urgência de medidas mitigatórias ao risco oferecido pelo achado assim o exigirem. Para esse fim uma listagem de, pelos menos, 3 (três) contatos telefônicos serão fornecidos para a CONTRATADA na fase de Inserção da CONTRATADA
b) por meio de uma Console de CTI que facilite consultas previamente cadastradas, sob demanda, periódicas, manuais e avulsas
c) por meio de Relatório Técnico semanal com informações objetivas, em arquivo pdf.
d) por meio de Relatório Executivo mensal com informações analíticas, como padrões de ameaças, tendências e pontos de atenção para a organização

2.7.11.12. Os reportes relativos à primeira forma, subitem “a” do item 2.7.11.11, deverão ser fornecidos, no mínimo, nos seguintes contextos:

a) Intenções de ataques que afetem os ambientes da ANAC.
b) Intenções de ataques que tenham como objetivo os ativos de informação monitorados ou a área de atuação da CONTRATANTE.

c) Campanhas relevantes de “hacktivismo”, como por exemplos ataques crescentes cujos alvos são, em sua maioria, órgão públicos ou de governo, ou ainda campanhas de ataques em que a vulnerabilidade explorada possa estar presente nas tecnologias implantadas na ANAC, bem como as campanhas de "hacktivismo" que tenham como alvo a área de atuação da ANAC, ou seja, ataques direcionados contra o setor da aviação civil em geral.
d) Intenção de executar atividades fraudulentas, ou mesmo aquelas já em curso, relacionadas aos recursos pesquisados.
e) Pessoas envolvidas em atividades criminosa, contraventora ou imoral contra a ANAC e sua área de atuação.
f) Códigos maliciosos (malwares) direcionados contra os ativos de informação monitorados.
g) Discussões online que divulguem de forma primária ou repliquem informações que possam ser utilizadas para executar ataques cibernéticos, inclusive engenharia social e ciberextorsão, contra qualquer dos ativos de informação monitorados.

3. **ESPECIFICAÇÃO DOS SERVIÇOS DE TESTE DE INVASÃO- LOTE 03**

3.1. A CONTRATADA deverá prover, tanto à infraestrutura quanto às aplicações atualmente implementados na ANAC, mecanismo de Teste de Invasão capaz de explorar as vulnerabilidades identificadas.

3.2. Para o serviço foram estimados 240 (duzentos e quarenta) alvos a serem utilizados, segundo interesse e necessidade da ANAC, ao longo da vigência do contrato a ser estabelecido com a CONTRATADA. Deverão ser considerados testes gray-box para fins de precificação.

3.3. Dos sistemas existentes hoje, estima-se que a ANAC irá demandar, no mínimo, 1 serviço por mês, conforme relação de serviços descrita para o Grupo 3 no Anexo III - Catálogo de Serviços.

3.4. Cada demanda solicitada poderá ter um ou mais alvos como objetivo destaque.

3.5. A atividade de Testes de Invasão poderá ser do tipo Externo e/ou Interno e terá como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações.

3.6. Para a realização dos testes de invasão, deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

3.6.1. OSSTMM 3 (The Open-Source Security Testing Methodology Manual).

3.6.2. ISSAF/PTF (Information Systems Security Assessment Framework).

3.6.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment).

3.6.4. NIST Special Publication 800-42 (Guideline on Network Security Testing).

3.6.5. OWASP TESTING GUIDE 4.0 - The Open Web Application Security Project.

3.7. Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos.

3.8. Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização dos mesmos serão, necessariamente, via "tickets” abertos.

3.9. A CONTRATADA deverá observar que os testes de invasão terão âmbito interno (qualquer ponto da rede corporativa da ANAC) quanto externo (através da Internet). Ambas as modalidades poderão ser realizadas remotamente.

3.10. Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério da CONTRATANTE.

3.11. Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

3.12. O teste de invasão deverá obedecer às seguintes fases:

3.12.1. Planejamento.

3.12.2. Descoberta.

3.12.3. Ataque.

3.12.4. Relatório Teste de Invasão.

3.12.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

3.12.6. Reavaliação, novo teste pós remediação.

3.12.6.1. A reavaliação não será contabilizada como uma nova atividade, devendo ser considerada como elemento do teste.

3.12.7. Relatório Final do Teste de Invasão.

3.13. Planejamento:

3.13.1. Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):

3.13.2. Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista).

3.13.3. Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste).

3.13.4. Técnica da caixa cinza ou híbrida (conhecimento limitado sobre o alvo).

3.14. Descoberta:

3.14.1. A fase de Descoberta, que tem como objetivo a obtenção de informações relevantes dentro do escopo do teste que possibilitam reconhecer possíveis ameaças/vulnerabilidades. Importante frisar que esta fase não deve se restringir à utilização de ferramentas automatizadas, sendo esperada atuação manual da equipe técnica contratada, aprofundando a análise da superfície de ataque à procura de vulnerabilidades não facilmente identificáveis. Deverão ser realizadas, no mínimo, as seguintes atividades:

3.14.2. Coleta passiva, caracterizada pela obtenção de informações utilizando-se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis:

3.14.2.1. Whois e nslookup (consultas DNS).
3.14.2.2. Sites de busca.
3.14.2.3. Listas de discussão.
3.14.2.4. Blogs de colaboradores.
3.14.2.5. Informações livres.
3.14.2.6. Captura de banner.
3.14.2.7. Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas, quando aplicáveis:
3.14.2.8. Port scanning (Mapeamento de rede).
3.14.2.9. Varredura de vulnerabilidade, que deverá verificar/identificar no mínimo:
3.14.2.9.1. Hosts ativos na rede.
3.14.2.9.2. Portas e serviços em execução.
3.14.2.9.3. Serviços ativos e vulneráveis nos hosts.
3.14.2.9.4. Fingerprinting de Sistemas operacionais dos hosts.
3.14.2.9.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas.
3.14.2.9.6. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional.
3.14.2.9.7. Identificação de vetores de ataque e cenários para exploração.
3.14.2.9.8. Vulnerabilidades Detectadas (CVE), classificadas com alto, médio ou Baixo Risco.
3.14.2.10. Em relação a serviços e aplicações web, deve-se ter/verificar:
3.14.2.10.1. Uso indevido de sistema de arquivos e arquivos temporários.
3.14.2.10.2. Evasão de informação por configurações padrão de tratamento de erros.
3.14.2.10.3. Tratamento indevido de entrada.
3.14.2.11. Problemas relacionados à má configuração dos serviços.
3.14.2.12. Gerenciamento inseguro de sessões web.

3.15. Ataque:

3.15.1. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

3.15.2. Deverá realizar testes de vulnerabilidades e invasão em endereços IP's, URL´s, aplicações, ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao teste de invasão.

3.15.3. Deverão ser aplicados, no mínimo, os seguintes tipos de ataques:

3.15.3.1. Violações do protocolo HTTP.
3.15.3.2. SQL Injection.
3.15.3.3. LDAP Injection.
3.15.3.4. Cookie Tampering.
3.15.3.5. Cross-Site Scripting (XSS).
3.15.3.6. Directory Transversal.
3.15.3.7. Buffer Overflow.
3.15.3.8. OS Command Execution.
3.15.3.9. Command Injection.
3.15.3.10. Remote Code Inclusion.
3.15.3.11. Server Side Includes (SSI) Injection.

3.15.3.12. File disclosure.
3.15.3.13. Information Leak.
3.15.3.14. Zero day attacks.
3.15.3.15. DDos (Distribuited Denial of Service).
3.15.3.16. Dos (Denial of Service).
3.15.3.17. Contra protocolo TCP.
3.15.3.18. Ataques contra a aplicação.

3.15.4. Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:
3.15.4.1. Bugs em serviços, aplicativos e sistemas operacionais.
3.15.4.2. SYN flooding.
3.15.4.3. Fragmentação de pacotes de IP.
3.15.4.4. Smurf e fraggle.
3.15.4.5. Teardrop, nuke e land.

3.15.5. Para ataques contra o protocolo TCP:
3.15.5.1. Sequestro de conexões.
3.15.5.2. Prognóstico de número de sequência do protocolo TCP.
3.15.5.3. Ataque de Mitnick.
3.15.5.4. Source routing.

3.15.6. Para ataques em nível da aplicação:
3.15.6.1. Buffer Overflow.
3.15.6.2. SNMP.
3.15.6.3. Vírus, worms e cavalos de Tróia.
3.15.6.4. Injeção de Código:
3.15.6.5. Ataques XSS (Cross-site Script).
3.15.6.6. Comprometimento do acesso remoto.
3.15.6.7. Manutenção de acesso.
3.15.6.8. Cobertura de rastros da invasão.

3.15.7. Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, os seguintes testes baseados na publicação OWASP TESTING GUIDE (The Open Web Application Security Project) em sua versão mais recente.

3.16. Relatório

3.16.1. Após a fase de Exploração, será elaborado um relatório do teste de intrusão com as seguintes informações:
3.16.1.1. Escopo, tipo e modalidade do teste.
3.16.1.2. Metodologias, técnicas, fontes de pesquisa e referências.
3.16.1.3. Atividades realizadas, em ordem cronológica.
3.16.1.4. Informações acessadas e detalhes da infraestrutura descoberta (caso aplicável).
3.16.1.5. Confirmação ou refutação de existência das vulnerabilidades.
3.16.1.6. Descrição de todas as vulnerabilidades e ameaças porventura encontradas, informando, no mínimo:
3.16.1.6.1. Nome.
3.16.1.6.2. Nível de Risco (Criticidade).
3.16.1.6.3. Intrusiva (sim / não).
3.16.1.6.4. Descrição.
3.16.1.6.5. Documentações do fabricante referente a vulnerabilidade, se houver.
3.16.1.6.6. Melhor prática para correção ou diminuição do risco.
3.16.1.6.7. Link do patch ou da correção se houver.
3.16.1.6.8. Número CVE, se houver.
3.16.1.6.9. Total de Vulnerabilidades.

3.16.2. Evidências da exploração das vulnerabilidades porventura encontradas.
3.16.3. Avaliação de riscos e impacto da vulnerabilidade e consequente exploração.
3.16.4. Contramedidas para correção ou mitigação dos riscos decorrentes das vulnerabilidades encontradas se houver.

Anexo ao Termo de Referência

Ambiente Tecnológico

1. AMBIENTE TECNOLÓGICO DA ANAC

1.1. Soluções de segurança

Site	Tipo	Marca	Modelo	Qtde
DF – Sede	Firewall de rede	CheckPoint	6900 Next Generation Threat Prevention & SandBlast (NGTX) Appliance	2
	Gerência da solução de Firewall	CheckPoint	Smart-1 5050 Next Generation Security Management (Virtual)	1
	WAF - Web Application Firewall	F5	BIG-IP i5800 HW com: • Licenciamento Best Bundle • Licença Ip Intelligence	2
	Gerência da solução WAF	F5	Ferramenta de gerência do BIG-IP – F5	1
DF – Centro de Treinamento	Firewall de rede	CheckPoint	6900 Next Generation Threat Prevention & SandBlast (NGTX) Appliance	2
	WAF - Web Application Firewall	F5	BIG-IP i5800 HW com: • Licenciamento Best Bundle • Licença Ip Intelligence	2
RJ	Firewall de rede	CheckPoint	6600 Next Generation Threat Prevention & SandBlast (NGTX) Appliance	2
SP	Firewall de rede	CheckPoint	6600 Next Generation Threat Prevention & SandBlast (NGTX) Appliance	2
SP-SJC	Firewall de rede	CheckPoint	6600 Next Generation Threat Prevention & SandBlast (NGTX) Appliance	2
			TOTAL	**16**

ANAC	Solução de EDR	CheckPoint	Harmony Endpoint	2000

1.2. Solução de ITSM

1.2.1. CITSMART

2. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

2.1. As informações abaixo dizem respeito ao parque tecnológico da Anac e servem como subsídio para a definição das propostas referentes aos itens:

2.1.1. Item 2 - Gestão de Ativos e Configuração Segura;

2.1.2. Item 3 - Gestão de Conta, Controle de Acesso e Auditoria;

2.1.3. Item 10 - Segurança de Aplicação

2.2. Soluções e serviços de segurança:

- Microsoft Defender
- Microsoft 365 E3 + EMS (Enterprise Mobility Security)
- Microsoft MFA ativo para todos os usuários
- Exchange Online Protection
- TeamPass (gerenciador de senhas)
- RackTables
- Solução de backup (NetBackup Appliance 5240)
- Backup off-site (Serviço de ObjectStorage – Dataprev)
- Serviço de AntiDDOS (Volumétrico) com operadora de internet
- Elasticsearch Security
- SonarQube
- OpenVAS
- Harbor (scanner Clair) – Kubernetes
- Varonis (DatAdvantage, DatAlert, DataPrivilege)
- Yara – Threat Hunting

2.3. Informações gerais:

Item	Qtd de ativos
Caixas de correio eletrônico (usuários)	1930
Contas de usuários	2342
Estações de trabalho / notebooks	2387
Access Points	66
Gateways de voz	8
Impressoras	34
Ativos de rede	150
Storage	2
Solução de backup	2
Servidores físicos de virtualização -MS Hyper-V	16
Servidores físicos de virtualização - Oracle	2
Servidores virtuais Windows	380
Servidores virtuais Linux	300
Servidores virtuais Oracle	14

Solução SD-WAN	14
Links de comunicação (internet, MPLS e infovia)	25

Anexo ao Termo de Referência

Catálogo de Serviços

Lote	Torre de Serviços	Serviço
1	Apoio à Gestão de Segurança	Realizar Assessment de Segurança da Informação
1	Apoio à Gestão de Segurança	Revisar Assessment de Segurança da Informação
1	Apoio à Gestão de Segurança	Elaborar Parecer de segurança da Informação
1	Apoio à Gestão de Segurança	Elaborar Política de Segurança da Informação
1	Apoio à Gestão de Segurança	Atualizar Política de Segurança da Informação
1	Apoio à Gestão de Segurança	Elaborar Diretrizes de Segurança da Informação
1	Apoio à Gestão de Segurança	Atualizar Diretrizes de Segurança da Informação
1	Apoio à Gestão de Segurança	Elaborar Cartilha de Segurança da Informação
1	Apoio à Gestão de Segurança	Atualizar Cartilha de Segurança da Informação
1	Apoio à Gestão de Segurança	Elaborar Relatório de Situação Semanal do PPSI
1	Apoio à Gestão de Segurança	Elaborar Relatório de Conformidade
1	Monitoramento e Gestão de Incidentes de Segurança	Monitorar ambiente cibernético da Anac
1	Monitoramento e Gestão de Incidentes de Segurança	Administração rotineira - Solução de TI - SIEM
1	Monitoramento e Gestão de Incidentes de Segurança	Elaborar Relatório Técnico para coleta de log
1	Monitoramento e Gestão de Incidentes de Segurança	Criar Painel Ativos com Log instrumentado na ferramenta de SIEM
1	Monitoramento e Gestão de Incidentes de Segurança	Atualizar Painel Ativos com Log instrumentado na ferramenta de SIEM
1	Monitoramento e Gestão de Incidentes de Segurança	Criar alerta de segurança
1	Monitoramento e Gestão de Incidentes de Segurança	Alterar alerta de segurança
1	Monitoramento e Gestão de Incidentes de Segurança	Criar ação de remediação automatizada
1	Monitoramento e Gestão de Incidentes de Segurança	Alterar ação de remediação automatizada
1	Monitoramento e Gestão de Incidentes de Segurança	Participar de exercício de resposta a incidente
1	Monitoramento e Gestão de Incidentes de Segurança	Realizar análise pós-incidente
1	Gestão de Ativos e Configuração Segura	Criar script de coleta de informações de ativo
1	Gestão de Ativos e Configuração Segura	Alterar script de coleta de informações de ativo
1	Gestão de Ativos e Configuração Segura	Criar alerta de inconformidade de configuração de ativo
1	Gestão de Ativos e Configuração Segura	Alterar alerta de inconformidade de configuração de ativo
1	Gestão de Ativos e Configuração Segura	Criar script de remediação de alteração configuração de ativo

1	Gestão de Ativos e Configuração Segura	Alterar script de remediação de alteração configuração de ativo
1	Gestão de Ativos e Configuração Segura	Criar painel de gestão do ativo
1	Gestão de Ativos e Configuração Segura	Atualizar painel de gestão do ativo
1	Gestão de Ativos e Configuração Segura	Cadastrar manualmente ativo
1	Gestão de Ativos e Configuração Segura	Atualizar manualmente informações do ativo
1	Gestão de Ativos e Configuração Segura	Criar alerta de detecção de ativo não autorizado
1	Gestão de Ativos e Configuração Segura	Atualizar alerta de detecção de ativo não autorizado
1	Gestão de Ativos e Configuração Segura	Realizar análise de impacto nos Ativos
1	Gestão de Ativos e Configuração Segura	Elaborar Documentação para Configuração Segura de Ativo
1	Gestão de Ativos e Configuração Segura	Atualizar Documentação para Configuração Segura de Ativo
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar Painel de Gestão de Contas e Controle de Acesso
1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar o painel de gestão de contas de usuário e controle de acesso
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar painel de serviço por sistema de identidade
1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar painel de serviço por sistema de identidade
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar painel de permissões por usuário
1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar painel de permissões por usuário
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar rotina de extração de dados de contas de usuário e acessos de serviço de identidade
1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar rotina de extração de dados de contas de usuário e acessos de serviço de identidade
1	Gestão de Conta, Controle de Acesso e Auditoria	Coletar logs de auditoria manualmente
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar rotina de desativação de conta
1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar rotina de desativação de conta
1	Gestão de Conta, Controle de Acesso e Auditoria	Criar rotina de revogação de acesso

1	Gestão de Conta, Controle de Acesso e Auditoria	Atualizar rotina de revogação de acesso
1	Gestão de Vulnerabilidades	Realizar varredura automatizada em ativos institucionais internos
1	Gestão de Vulnerabilidades	Realizar varredura automatizada em ativos institucionais externos
1	Gestão de Vulnerabilidades	Criar painel de situação de atualização dos ativos
1	Gestão de Vulnerabilidades	Atualizar painel de situação de atualização dos ativos
1	Gestão de Vulnerabilidades	Criar rotina de extração de dados das versões instalada dos ativos
1	Gestão de Vulnerabilidades	Atualizar rotina de extração de dados das versões instalada dos ativos
1	Gestão de Vulnerabilidades	Criar painel de situação da versão dos ativos por CVEs
1	Gestão de Vulnerabilidades	Atualizar painel de situação da versão dos ativos por CVEs
1	Gestão de Vulnerabilidades	Criar rotina de extração de CVEs para os ativos
1	Gestão de Vulnerabilidades	Atualizar rotina de extração de CVEs para os ativos
1	Gestão de Vulnerabilidades	Apoiar na Elaboração de estratégia de remediação
1	Gestão de Vulnerabilidades	Apoiar na Atualização de estratégia de remediação
1	Segurança de Redes	Atender requisições do portal de serviços - SLA 2 horas
1	Segurança de Redes	Atender requisições do portal de serviços - SLA 4 horas
1	Segurança de Redes	Atender requisições do portal de serviços - SLA 8 horas
1	Segurança de Redes	Atender requisições do portal de serviços - SLA 16 horas
1	Segurança de Redes	Atender requisições do portal de serviços - SLA 70 horas
1	Segurança de Redes	Apoiar na Simulação do Procedimento Operacional de Recuperação de Serviço ou Solução de TI
1	Segurança de Redes	Analisar, propor e executar correção para problemas no ambiente de TI
1	Segurança de Redes	Desenvolver o relatório técnico Operacional (primeira versão)
1	Segurança de Redes	Desenvolver melhorias para o relatório técnico Operacional
1	Segurança de Redes	Elaborar o Relatório técnico Operacional (conforme padrão do mês anterior)
1	Segurança de Redes	Administração rotineira - Acesso Remoto (VPN SSL)
1	Segurança de Redes	Administração rotineira - EndPoint de Segurança (EDR)
1	Segurança de Redes	Administração rotineira - Extranet (VPN Site-to-Site)
1	Segurança de Redes	Administração rotineira - Infraestrutura de Firewall/IPS
1	Segurança de Redes	Administração rotineira - Serviço AAA (Radius, NPS)
1	Segurança de Redes	Administração rotineira - Instalação de patches e atualizações
1	Segurança de Redes	Planejar e executar demanda específicas
1	Segurança de Redes	Administração rotineira - WAF
1	Segurança de Aplicação	Administração rotineira - SAST
1	Segurança de Aplicação	Administração rotineira - DAST
1	Segurança de Aplicação	Administração rotineira - Dependency Scanning
1	Segurança de Aplicação	Administração rotineira - Container Scanning
1	Segurança de Aplicação	Administração rotineira - Secrets Detection
1	Segurança de Aplicação	Realizar Inspeção de segurança de Código-fonte
1	Segurança de Aplicação	Realizar Inspeção de segurança de Servidor de Aplicação
1	Segurança de Aplicação	Realizar Inspeção de segurança de Solução em Container

Lote	Torre de Serviços	Serviços
2	Inteligência de Ameaças	Monitorar surface web, deep web e dark web (Pessoas de Interesse)
2	Inteligência de Ameaças	Monitorar da surface web, deep web e dark web (Produtos/Marcas)
2	Inteligência de Ameaças	Monitorar Sites e contas fraudulentas
2	Inteligência de Ameaças	Monitoração de fontes de informações (Domínios/subdomínios)
2	Inteligência de Ameaças	Monitorar de vazamento de informações (Nomes de Empresas Fornecedoras)

Lote	Torre de Serviços	Serviços
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Externo
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Interno
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Aplicação Web
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - API
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Aplicativo Móvel
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Redes sem fio
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Engenharia Social
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Redes
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Nuvem
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Máquina do Usuário
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Ransomware
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Banco de Dados
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Acesso Remoto
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Phishing
3	Testes de Invasão	Realizar Teste de Invasão (Pentest) - Física

Anexo ao Termo de Referência

Termo de Compromisso de Manutenção de Sigilo

Agência Nacional de Aviação Civil

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO
O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não. **Referência: Art. 18, Inciso V, alínea "a" da IN SGD/ME Nº 94/2022.**

Pelo presente instrumento a ANAC - Agência Nacional de Aviação Civil, sediada no Setor Comercial Sul, Quadra 9, Lote C, Edifício Parque Cidade Corporate, Torre A, Brasília-DF, CEP 70.308-200, CNPJ n° 07.947.821/0001-89, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA**;
CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;
CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;
Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

[...]

[...]

[...]

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

[...]

[...]

[...]

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

[...]

[...]

[...]

4 – DOS LIMITES DO SIGILO

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

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

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.

[...]
[...]
[...]

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face

da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

[...]

[...]

[...]

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

[...]

7 – PENALIDADES

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 PRINCIPAL 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 CONTRATANTE, 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 previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

[...]
[...]
[...]

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – 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;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

[...]
[...]
[...]

9 – FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

[...]

10 – ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	**GESTOR DO CONTRATO**
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx
TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.

Anexo ao Termo de Referência

Termo de Ciência

Agência Nacional de Aviação Civil

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	**CNPJ**	xxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	**Matrícula**	**Assinatura**
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
…	…	…

<Local>, <dia> de <mês> de <ano>.

Anexo ao Termo de Referência

Ordem de Serviço

Agência Nacional de Aviação Civil

ORDEM DE SERVIÇO OU DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	**E-mail**	xxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	**Descrição do bem ou serviço**	**Métrica**	**Valor unitário (R$)**	**Qtde/Vol.**	**Valor Total (R$)**
1	...	...	...	...	...
...	...	...	...	...	...

Valor total estimado da OS/OFB	

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS/OFB> <Ex.: Contatar a área solicitante para agendamento do horário de entrega> <Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	**Data do Fim:**	<dd/mm/aaaa>

CRONOGRAMA DE EXECUÇÃO/ENTREGA

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	**A serem gerados e/ou atualizados**

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

_____

<Nome >

<Responsável pela demanda/

Fiscal Requisitante>

Matr.: <Nº da matrícula>

_____

<Nome >

Gestor do Contrato

Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx

Anexo ao Termo de Referência

Termo de Recebimento Provisório de Serviços

Agência Nacional de Aviação Civil

TERMO DE RECEBIMENTO PROVISÓRIO – SERVIÇOS DE TIC

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXX

Agência Nacional de Aviação Civil

TERMO DE RECEBIMENTO PROVISÓRIO – SERVIÇOS DE TIC

INTRODUÇÃO
O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OS de abertura>	<Ex.: PF>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à <OS> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e <atende(m)/atende(m) parcialmente/não atende(m)> às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, 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**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – ASSINATURA

FISCAL TÉCNICO

_____

<Nome do Fiscal Técnico do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

PREPOSTO

_____
<Nome do Preposto do Contrato>
Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

Anexo ao Termo de Referência

Termo de Recebimento Definitivo

Agência Nacional de Aviação Civil

TERMO DE RECEBIMENTO DEFINITIVO

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1.0	Primeira versão do documento.	XXXXXXXXXXXX

Agência Nacional de Aviação Civil

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos. **Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do

Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
...	...	...	.....
...	...	...	.....
...	...	...	.....

4 – 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 <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

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

5 – ASSINATURA

GESTOR DO CONTRATO

_____

<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

5 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO
Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima. _____ <Nome do Gestor do Contrato> **Matrícula:** xxxxxxxx <Local>, <dia> de <mês> de <ano>

7 – CIÊNCIA
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxxx <Local>, <dia> de <mês> de <ano>

Anexo ao Termo de Referência

Modelo de Proposta Comercial

ANEXO IX do Termo de Referência

MODELO DE PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

Identificação da Licitação

Nº do Processo

Nº da Licitação

Nome da Empresa

CNPJ

GRUPO XX - <descrição do grupo>

ITEM XX - <descrição do Item>

Componentes de Custo de Pessoal

Identificação do Perfil Profissional	Salário (S)	Fator K (K)	Custo total por perfil (CT= S x K)	Qtde. profissionais por perfil (Q)	Custo Mensal por Perfil (CM = CT x Q)

Subtotal componentes de custo de Pessoal

Demais Componentes de Custo

Descrição	Memória de Cálculo / Justificativa	Valor Mensal
Custos com software		
Custos com recursos de computação		
Custos com equipamentos		
Custos com serviços de informações		
Outros custos (especificar)		
Subtotal Demais componentes de custo		

Componentes de Preço (não compreendidos na composição do Fator K)

Descrição	Valor Mensal

Elementos Comerciais (Fatores/Ajustes Comerciais)

Cobertura Tributária

Outros componentes (especificar)

Subtotal componentes de preço

Total Mensal:

Valor Total do [item/grupo]: **[Valor mensal x quantidade de meses previstos para contratação]**

Assim sendo, o valor total da proposta é de R$ _____ **(por extenso).**

A presente proposta é baseada nas especificações, condições e prazos estabelecidos no edital de Pregão nº ___/2025-ANAC, os quais nos comprometemos a cumprir integralmente.

Prazo de validade da proposta: _____ dias (não inferior a sessenta dias)

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

Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos.

Dados da empresa:

Razão Social		CNPJ (MF) nº	
Inscrição Estadual nº		Inscrição Municipal nº	
Endereço			
Telefone		Fax	
Cidade:		UF	

Dados do Representante para fim de apresentação da proposta e assinatura do contrato:

Nome			
Cargo/Função		Nacionalidade	
Endereço			
Telefone			
Endereço Eletrônico			

Local e data

_____

Assinatura e carimbo

(Representante Legal)

Anexo ao Termo de Referência

Declaração de Responsabilidade

DECLARAÇÃO DE RESPONSABILIDADE

PREGÃO Nº ___/202

Eu, ___, na qualidade de Responsável Legal da Empresa ___, declaro que esta empresa decide por não realizar a vistoria técnica e está ciente ser da sua responsabilidade a ocorrência de eventuais prejuízos em virtude da não verificação dos locais de execução dos serviços, estando, em nome da empresa de acordo com as condições gerais e específicas estabelecidas nesta licitação, para todos os efeitos legais, às quais a empresa se submete incondicional e integralmente, não cabendo alegações, pela supracitada empresa, em qualquer época, de desconhecimento de estado, fatos e detalhes que impossibilitem ou dificultem a execução dos serviços ou o cumprimento de todas as suas obrigações.

Declaro que a empresa está apta a iniciar os serviços imediatamente após a assinatura do contrato a ser firmado, se o objeto da licitação, porventura, lhe for adjudicada.

Local, ___, de _____ de 2023.

Assinatura e nome do representante da empresa

MODELO DE TERMO DE CONTRATO
Lei nº 14.133, de 1º de abril de 2021

ANEXO II ao Edital

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

(Processo Administrativo n°00058.007264/2023-23)

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI A AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL E .....

A Agência Nacional de Aviação Civil, com sede no(a) Setor Comercial Sul, Quadra 09, Lote C, Ed. Parque Cidade Corporate, Torre A, 3º andar, na cidade de Brasília/DF inscrito(a) no CNPJ sob o nº 07.947.821/0001-89, neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ....., de ..... de ..... de 20..., publicada no *DOU* de ..... de ..... de ....., portador da Matrícula Funcional nº ....., doravante denominado CONTRATANTE, e o(a) ....., *inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em .....* doravante designado CONTRATADO, *neste ato representado(a) por* ..... (nome e função no contratado), *conforme atos constitutivos da empresa **OU** procuração apresentada nos autos,* tendo em vista o que consta no Processo nº 00058.007264/2023-23 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente *do Pregão Eletrônico n. .../2024*, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO (ART. 92, I E II)

1.1. O objeto do presente instrumento é a contratação de serviços técnicos especializados de Segurança da Informação para a implantação de um Security Operation Center - SOC, envolvendo a prestação de serviços de gerenciamento, monitoramento, detecção e resposta a incidentes de segurança, de gestão de vulnerabilidades, de gestão de ativos e configuração segura, de gestão de conta, controle de acesso e auditoria, de apoio à gestão de segurança, serviços de inteligência de ameaças cibernéticas e de testes de invasão, pelo período de 24 (vinte e quatro meses) meses, na forma de serviços continuados, executados sem dedicação exclusiva de mão de obra, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

Tabela 1

Grupo	Item	Especificação	CATSER	Unidade de Medida	Quantidade	Valor Unitário	Valor Total
1	1	Apoio à Gestão de Segurança	27014	Mensal	24 meses		
1	2	Gestão de Ativos e Configuração Segura	27014	Mensal	24 meses		
1	3	Gestão de Conta, Controle de Acesso e Auditoria	27014	Mensal	24 meses		
1	4	Gestão de incidentes de segurança da informação (Blue Team)	27014	Mensal	24 meses		
1	5	Monitoramento e correlação de eventos de segurança da informação	27014	Mensal	24 meses		

1	6	Serviço de contratação de pacotes adicionais de 500 EPS da ferramenta SIEM por 12 meses	27014	Sob demanda	10		
1	7	Gestão de vulnerabilidades	27014	Mensal	24 meses		
1	8	Solução de gerenciamento de vulnerabilidades de segurança	27014	Mensal	24 meses		
1	9	Segurança de Redes	27014	Mensal	24 meses		
1	10	Segurança de Aplicação	27014	Mensal	24 meses		
2	11	Inteligência de Ameaças Cibernéticas	27014	Mensal	24 meses		
3	12	Testes de Invasão	27014	Sob demanda	240		
Total							

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados da data de assinatura pelo CONTRATANTE, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes.

2.1.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.1.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.1.4. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.1.5. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (ART. 92, IV, VII E XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não é admitida a subcontratação do objeto contratual, exceto para a prestação de serviços de "*remote hands*", relacionados ao item 9 do Grupo 1, Segurança de Redes, para atividades que demandem intervenção presencial, como acompanhamento presencial de fornecedor de suporte, manutenções de equipamentos e substituição de peças.

4.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral do contratado pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

4.3. A subcontratação depende de autorização prévia do contratante, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

4.4. O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

4.5. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R$..... (.....)

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA - PAGAMENTO (ART. 92, V E VI)

6.1. O prazo para pagamento e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE (ART. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 04/11/2024.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade .

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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

7.7. 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.

7.8. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (ART. 92, X, XI E XIV)

8.1. São obrigações do Contratante, além das previstas no termo de referência:

8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.6. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

8.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

8.11. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

8.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.14. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.15. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (ART. 92, XIV, XVI E XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no Termo de Referência:

9.2. Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.

9.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.4. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados ;

9.5. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.7. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

9.8. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.9. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.10. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

9.11. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

9.12. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

9.13. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.14. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.15. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.16. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

9.17. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.18. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.19. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

9.20. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

9.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.22. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

9.23. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

9.24. Realizar os serviços de manutenção e assistência técnica no(s) seguinte(s) local(is) indicados no Termo de referência;

9.24.1. O técnico deverá se deslocar ao local da repartição, quando necessário, e nas condições definidas no Termo de Referência.

9.25. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços.

9.26. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

9.26.1. Considerando que o projeto contratado se refere a obra imaterial de caráter tecnológico, insuscetível de privilégio, a cessão dos direitos a que se refere o subitem acima inclui o fornecimento de todos os dados, documentos e elementos de informação pertinentes à tecnologia de concepção, desenvolvimento, fixação em suporte físico de qualquer natureza e aplicação da obra.

10. CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

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

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

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

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

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

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive

quanto a eventual descarte realizado.

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

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

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

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

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (ART. 92, XII)

11.1. O contratado apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou, ainda, pela fiança bancária, em valor correspondente a 5% (cinco por cento) do valor ~~inicial/~~ total ~~/anual~~ do contrato.

11.2. Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.3. Caso utilizada a modalidade de seguro-garantia, a apólice deverá ter validade durante a vigência do contrato e ~~/OU~~ por 90 (noventa) dias após o término da vigência contratual, permanecendo em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

11.4. A apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

11.5. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 11.6 deste contrato.

11.6. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

11.7. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

11.7.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

11.7.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

11.7.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pelo contratado, quando couber.

11.8. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 11.7, observada a legislação que rege a matéria.

11.9. A garantia em dinheiro deverá ser efetuada em favor do contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

11.10. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

11.11. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.12. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia

deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

11.13. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 20 (vinte) dias úteis, contados da data em que for notificada.

11.14. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

11.14.1. O emitente da garantia ofertada pelo contratado deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11.14.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

11.15. Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do contratante, mediante termo circunstanciado, de que o contratado cumpriu todas as cláusulas do contrato;

11.16. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

11.17. O garantidor não é parte para figurar em processo administrativo instaurado pelo contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

11.18. O contratado autoriza o contratante a reter, a qualquer tempo, a garantia, na forma prevista no Edital e neste Contrato.

11.19. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (ART. 92, XIV)

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a. der causa à inexecução parcial do contrato;
b. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c. der causa à inexecução total do contrato;
d. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f. praticar ato fraudulento na execução do contrato;
g. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
iv. **Multa**

1. Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela

inadimplida, até o limite de 30 (trinta) dias;

2. Moratória de 0,5% (cinco décimos por cento) do valor total do contrato por dia de atraso injustificado, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

    a. O atraso superior 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

3. Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 12.1, de 1% a 10% do valor do Contrato.
4. Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 12.1, de 1% a 10% do valor do Contrato.
5. Para infração descrita na alínea "b" do subitem 12.1, a multa será de 0,5% a 10% do valor do Contrato.
6. Para infrações descritas na alínea "d" do subitem 12.1, a multa será de 0,5% a 5% do valor do Contrato.
7. Para a infração descrita na alínea "a" do subitem 12.1, a multa será de 0,5% a 5% do valor do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a. a natureza e a gravidade da infração cometida;
b. as peculiaridades do caso concreto;
c. as circunstâncias agravantes ou atenuantes;
d. os danos que dela provierem para o Contratante;
e. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.10. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de

direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

12.12. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

12.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.14. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (ART. 92, XIX)

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).

13.8. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (ART. 92, VIII)

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

i. Gestão/Unidade:
ii. Fonte de Recursos:
iii. Programa de Trabalho:
iv. Elemento de Despesa:
v. Plano Interno:
vi. Nota de Empenho:

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (ART. 92, III)

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

18. CLÁUSULA DÉCIMA OITAVA– FORO (ART. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal em Brasília - DF, Seção Judiciária de primeiro grau para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

[Local], [dia] de [mês] de [ano].

_____

Representante legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-