AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL
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

Processo nº 00058.007213/2018-34

PREGÃO ELETRÔNICO

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

PREGÃO ELETRÔNICO Nº 28/2019

(Processo Administrativo n.°00058.007213/2018-34**)**

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, CEP 70.308-200, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **com o critério de julgamento (menor preço por grupo)**, sob a forma de execução indireta, no regime de empreitada por preço unitário, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: **11/12/2019**

Horário: **10h**

Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (*Microsoft Active Directory*), correio eletrônico (*Microsoft Exchange Server*) e servidores de arquivos (*Microsoft File Server*). A solução deve monitorar os usuários em tempo real, identificar desvios de comportamento, permitir delegação de gerenciamento de acesso aos proprietários dos dados, executar ações proativas em múltiplos objetos, e identificar e classificar conteúdos sensíveis. A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formados por 6 (seis) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3. O critério de julgamento adotado será o menor preço GLOBAL do grupo, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

1.4. Cada serviço ou produto do lote 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, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB.

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2019, na classificação abaixo:

Gestão/Unidade: 20214

Fonte: 0174120069

Programa de Trabalho: 26.125.2017.2912.0001

Elemento de Despesa: 4.4.90.40-05; 3.3.90.40-10; 3.3.90.40-20

3. DO CREDENCIAMENTO

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumir 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 da senha, ainda que por terceiros.É de responsabilidade do cadastrado 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.

3.5. É de responsabilidade do cadastrado 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.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

4. DA PARTICIPAÇÃO NO PREGÃO.

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.2. Não poderão participar desta licitação os interessados:

4.2.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.2.2. que não atendam às condições deste Edital e seu(s) anexo(s);

4.2.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.2.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.2.5. que estejam sob falência, concurso de credores ou insolvência, em processo de dissolução ou liquidação;

4.2.6. entidades empresariais que estejam reunidas em consórcio;

4.2.7. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.2.8. instituições sem fins lucrativos (parágrafo único do art. 12 da Instrução Normativa/SEGES nº 05/2017)

4.2.8.1. É admissível a participação de organizações sociais, qualificadas na forma dos arts. 5º a 7º da Lei 9.637/1998, desde que os serviços objeto desta licitação se insiram entre as atividades previstas no contrato de gestão firmado entre o Poder Público e a organização social (Acórdão nº 1.406/2017- TCU-Plenário), mediante apresentação do Contrato de Gestão e dos respectivos atos constitutivos.

4.2.9. sociedades cooperativas, considerando a vedação contida no art. 10 da Instrução Normativa SEGES/MP nº 5, de 2017, bem como o disposto no Termo de Conciliação firmado entre o Ministério Público do Trabalho e a AGU.

4.3. Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a. detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou
b. de autoridade hierarquicamente superior no âmbito do órgão contratante.

4.3.1. Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto n.º 7.203, de 04 de junho de 2010);

4.4. Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.5. Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.5.1. 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.

4.5.1.1. 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 ou empresa de pequeno porte.

4.5.1.2. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.5.2. que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;

4.5.3. que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.5.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.5.5. que 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;

4.5.6. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.5.7. que não possui, em sua cadeia produtiva, 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;

4.5.8. que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.5.9. que cumpre os requisitos do Decreto n. 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.5.9.1. a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

4.6. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

5.2. O Envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art, 43, §1º, da LC nº 123, de 2006.

5.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

6. PREENCHIMENTO DA PROPOSTA

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

6.1.1. Valor unitário e total do item e do grupo*;*

6.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços, apurados mediante o preenchimento do modelo de Planilha de Custos e Formação de Preços, conforme anexo deste Edital;

6.3.1. A Contratada deverá 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, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1° do artigo 57 da Lei n° 8.666, de 1993.

6.3.2. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea "b" do inciso I do art. 65 da Lei n. 8.666/93 e nos termos do art. 63, §2° da IN SEGES/MPDG n. 5/2017.

6.4. A empresa é a única responsável pela cotação correta dos encargos tributários. Em caso de erro ou cotação incompatível com o regime tributário a que se submete, serão adotadas as orientações a seguir:

6.4.1. cotação de percentual menor que o adequado: o percentual será mantido durante toda a execução contratual;

6.4.2. cotação de percentual maior que o adequado: o excesso será suprimido, unilateralmente, da planilha e haverá glosa, quando do pagamento, e/ou redução, quando da repactuação, para fins de total ressarcimento do débito.

6.5. 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, devendo o licitante ou contratada apresentar ao pregoeiro ou à fiscalização, a qualquer tempo, comprovação da adequação dos recolhimentos, para os fins do previsto no subitem anterior.

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

6.7. 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 os serviços 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.

6.8. 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.

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

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

6.10.1. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo 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

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

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

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que **identifique o licitante.**

7.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

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

7.5. 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.

7.5.1. O lance deverá ser ofertado pelo valor total do item e do grupo.

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

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

7.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser **de 1 (um) mil reais**.

7.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

7.10. **Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto" em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.**

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

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

7.13. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.14. Encerrada a fase competitiva sem que haja prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.15. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia;

7.15.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

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

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

7.18. 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.

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

7.20. O Critério de julgamento adotado será o menor preço, conforme definido neste Edital e seus anexos.

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

7.22. 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 LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.23. 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.

7.24. A melhor classificada nos termos do item 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.

7.25. 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.

7.26. 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.

7.27. A ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação, de maneira que só poderá haver empate entre propostas iguais (não seguidas de lances).

7.27.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos serviços:

7.27.1.1. prestados por empresas brasileiras;

7.27.1.2. prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.27.1.3. prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.28. Persistindo o empate entre propostas, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.29. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor

preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das prevista deste Edital.

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

7.29.2. O pregoeiro solicitará ao licitante melhor 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.

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

7.31. Será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

7.31.1. 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.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

8.1. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade de preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no §9º do art. 26 do Decreto nº 10.024/2019.

8.2. Será desclassificada a proposta ou o lance vencedor, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG n. 5/2017, que:

8.2.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

8.2.2. contenha vício insanável ou ilegalidade;

8.2.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.2.4. apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), ou que apresentar preço manifestamente inexequível.

8.2.4.1. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

8.2.4.1.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.3. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MP N. 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.4. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.5. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.5.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata.

8.6. O Pregoeiro poderá convocar o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no "chat" prazo mínimo de **2 (duas) horas**, sob pena de não aceitação da proposta.

8.6.1. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

8.6.2. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.

8.7. Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.

8.8. O Pregoeiro analisará a compatibilidade dos preços unitários apresentados na Planilha de custos com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação;

8.9. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço proposto.

8.9.0.1. Considera-se erro no preenchimento da planilha a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, exceto para atividades de prestação de serviços previstas nos §§5º-B a 5º-E, do artigo 18, da LC 123, de 2006.

8.9.0.2. Em nenhuma hipótese poderá ser alterado o teor da proposta apresentada, seja quanto ao preço ou quaisquer outras condições que importem em modificações de seus termos originais, ressalvadas apenas as alterações absolutamente formais, destinadas a sanar evidentes erros materiais, sem nenhuma alteração do conteúdo e das condições referidas, desde que não venham a causar prejuízos aos demais licitantes;

8.10. 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.

8.11. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

8.12. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

8.13. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

9. DA HABILITAÇÃO

9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

9.1.1. SICAF;

9.1.2. Consulta consolidada de Pessoa Jurídica do Tribunal de Contas da União (http://certidoes-apf.apps.tcu.gov.br/);;

9.1.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as

sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.3.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.3.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.3.1.2. O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.4. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.5. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o terceiro dia útil anterior à data prevista para recebimento das propostas;

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (de duas) horas, sob pena de inabilitação.

9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto do item 5.3, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

9.8. **Habilitação jurídica:**

9.8.1. no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.8.2. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.3. inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

9.8.4. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.5. decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.6. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.9. **Regularidade fiscal e trabalhista:**

9.9.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

9.9.2. 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 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.9.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.9.4. 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;

9.9.5. prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6. prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7. caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal do seu domicílio ou sede, ou outra equivalente, na forma da lei;

9.10. **Qualificação Econômico-Financeira:**

9.10.1. certidão negativa de falência expedida pelo distribuidor da sede do licitante;

9.10.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

9.10.2.1. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.2. é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.10.3. comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

9.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação.

9.11. **Qualificação Técnica:**

9.11.1. As empresas, cadastradas ou não no SICAF, para todos os itens do grupo, deverão comprovar, ainda, a qualificação técnica, por meio do atendimento dos requisitos previstos no item 11.4 do Termo de Referência, Anexo I deste Edital, além de:

9.11.1.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com os serviços de suporte técnico e garantia (item 5 da contratação), por período não inferior a 1(um) ano, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

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

9.11.1.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MP n. 5, de 2017.

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

9.11.1.5. Deverá haver a comprovação da experiência mínima de 1 (um) ano na prestação dos serviços de suporte técnico e garantia, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os anos serem ininterruptos, conforme item 10.7.1 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.11.1.6. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da

contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MP n. 5/2017.

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.14. Caso a proposta mais vantajosa seja ofertada por microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.15. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa ou empresa de pequeno porte com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DA PROVA DE CONCEITO - TESTE DE CONFORMIDADE

10.1. O licitante detentor da proposta classificada em primeiro lugar, que atender a todos os requisitos de habilitação, será convocado para realizar Prova de Conceito.

10.2. A Prova de Conceito visa à aferição da real capacidade da Solução Tecnológica ofertada pelo licitante e será realizada conforme descrito no item 11.3 do Termo de Referência, Anexo ao presente Edital.

10.3. No caso de o licitante ofertante do melhor lance não passar na Prova de Conceito, o pregoeiro convocará o próximo licitante detentor de proposta válida, obedecida a classificação na etapa de lances, até que um licitante cumpra os requisitos previstos neste Edital e no Termo de Referência e seja declarado vencedor.

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 72 (setenta e duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

11.1.1. ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

11.1.2. apresentar a planilha de custos, devidamente ajustada ao lance vencedor;

11.1.3. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

11.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

11.2.1. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

11.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

11.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

11.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

11.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

11.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

12. DOS RECURSOS

12.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra quais decisões pretende recorrer e por quais motivos, em campo próprio do sistema.

12.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

12.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

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

12.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº

123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico (“chat”) e e-mail de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

14.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

15. DA GARANTIA DE EXECUÇÃO

15.1. Será exigida a prestação de garantia na presente contratação, conforme regras constantes do Termo de Referência

16. DO TERMO DE CONTRATO

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato.

16.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

16.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

16.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

16.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

16.3.2. a contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

16.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

16.4. O prazo de vigência da contratação é de 36 (trinta e seis) meses prorrogável conforme previsão no instrumento contratual.

16.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.5.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

16.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

16.6. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

16.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

17. DO REAJUSTAMENTO EM SENTIDO GERAL

17.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

18. DA RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

18.1. Os critérios de recebimento do objeto e de fiscalização estão previstos no Termo de Referência.

19. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

19.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

20. DO PAGAMENTO

20.1. As regras acerca do reajuste do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

21. DAS SANÇÕES ADMINISTRATIVAS.

21.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

21.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

21.1.2. apresentar documentação falsa;

21.1.3. deixar de entregar os documentos exigidos no certame;

21.1.4. ensejar o retardamento da execução do objeto;

21.1.5. não mantiver a proposta;

21.1.6. cometer fraude fiscal;

21.1.7. comportar-se de modo inidôneo;

21.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

21.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

21.3.1. Advertência por faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

21.3.2. Multa de 0,5% (meio por cento) sobre o valor estimado do Grupo prejudicado pela conduta do licitante;

21.3.3. Suspensão de licitar e impedimento de contratar com a Agência Nacional de Aviação Civil, pelo prazo de até dois anos;

21.3.4. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

21.3.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

21.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

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

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

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

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

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

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

21.11. As penalidades serão obrigatoriamente registradas no SICAF.

21.12. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

22. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

22.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

22.2. A impugnação **deverá** ser realizada, **exclusivamente,** por forma eletrônica, pelo e-mail **licitacao@anac.gov.br**

22.3. Caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação..

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

22.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

22.6. O pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contados da data do recebimento do pedido e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos

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

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

22.8. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração.

23. DAS DISPOSIÇÕES GERAIS

23.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

23.2. 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.

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

23.4. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

23.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

23.6. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

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

23.8. 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.

23.9. 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.

23.10. 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.

23.11. 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.

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

23.13. O Edital está disponibilizado, na íntegra, no endereço eletrônico www.comprasgovernamentais.gov.br, e também poderão ser lidos e/ou obtidos no endereço constante no preâmbulo deste edital, nos dias úteis, no horário das 8 horas às 17 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

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

23.14.1. ANEXO I - Termo de Referência (3673826);

23.14.2. ANEXO II - Minuta do Termo de Contrato (3673825);

23.14.3. Apêndice - Estudo Técnico Preliminar (ETP) - TIC GEIT (1897709).

Brasília, 29 de novembro de 2019.

Aderson de Lima Calazans

Pregoeiro Oficial

Documento assinado eletronicamente por **Aderson de Lima Calazans**, **Analista Administrativo**, em 28/11/2019, às 09:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sistemas.anac.gov.br/sei/autenticidade, informando o código verificador **3774887** e o código CRC **E2CDC12E**.

Referência: Processo nº 00058.007213/2018-34 SEI nº 3774887

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL
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

TERMO DE REFERÊNCIA

Processo nº 00058.007213/2018-34

1. DO OBJETO

1.1. Aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (*Microsoft Active Directory*), correio eletrônico (*Microsoft Exchange Server*) e servidores de arquivos (*Microsoft File Server*). A solução deve monitorar os usuários em tempo real, identificar desvios de comportamento, permitir delegação de gerenciamento de acesso aos proprietários dos dados, executar ações proativas em múltiplos objetos, e identificar e classificar conteúdos sensíveis. A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, conforme condições, quantidades e exigências estabelecidas neste instrumento.

Grupo	Item	Descrição / especificação	Unidade de medida	Quantidade
1	1	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft *Active Directory).*	Usuários	2.400
	2	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de servidores de arquivos.	Usuários	2.400
	3	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de correio eletrônico (*Microsoft Exchange).*	Usuários	2.400
	4	Licença perpétua de software de Solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis.	Usuários	2.400
	5	Serviços de suporte técnico e garantia	Meses	36
	6	Treinamento para as soluções contratadas	Turma	1

1.2. Conforme Decreto nº 8.538, de 2015, Art. 10, Parágrafo único, Inciso II, não foi considerada a reserva de cotas para microempresas e empresas de pequeno porte porque a natureza do bem ou serviço é incompatível com a aplicação dos benefícios.

1.3. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela acima.

1.4. A presente contratação adotará como regime de execução a empreitada por preço unitário.

1.5. O prazo de vigência do contrato é de 36 (trinta e seis) meses, podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, com base no artigo 57, II, da Lei 8.666/1993.

1.5.1. A prorrogação do contrato será referente apenas ao item 5 - "Serviços de suporte técnico e garantia".

1.5.2. O prazo de vigência é justificado pela necessidade de execução de atividades de análise de saúde do ambiente e aplicação de atualizações de forma periódica, além dos serviços garantia de funcionamento da solução contratada.

1.5.3. No tocante a esses serviços, cabe salientar que eles são de natureza continuada, tendo em vista a sua criticidade para o perfeito funcionamento das licenças que compõem Solução de Auditoria, e, consequentemente, evitar interrupções nas atividades da ANAC. Nessa linha de raciocínio, vale destacar o que dispõe, in verbis, a seguinte Orientação Normativa nº 38, de 13/12/2011, da AGU – Advocacia Geral da União – acerca da vigência dos contratos firmados pela Administração Pública Federal: "Orientação Normativa AGU nº 38, de 13/12/2011 Ementa: 'Nos contratos de prestação de serviços de natureza continuada, deve-se observar que: a) o prazo de vigência originário, de regra, é de até 12 meses; b) excepcionalmente, este prazo poderá ser fixado por período superior a 12 meses nos casos em que, diante da peculiaridade e/ou complexidade do objeto, fique tecnicamente demonstrado o benefício advindo para a administração; e c) é juridicamente possível a prorrogação do contrato por prazo diverso do contratado originariamente'. Referência: Art. 57, inciso II, da Lei n° 8.666/93; Parecer/AGU/NAJSP/n° 417/2009-MTU; Nota-Jurídica PGBC-7271/2009; Acórdãos TCU nº 1.858/2004 - Plenário e nº 551/2002-2ª Câmara." (Grifos nossos)

1.5.4. Nessa esteira de argumentos e raciocínio, justifica-se a necessidade de a vigência contratual ser, inicialmente, de 36 (trinta e seis) meses, prorrogáveis até o limite de 60 (sessenta) meses, nos termos do artigo 57, inciso II, da Lei nº 8.666/1993.
Obviamente que esse período diz respeito somente ao item relativo aos serviços de suporte técnico e garantia, dado seu caráter essencial à funcionalidade ininterrupta de toda a Solução e ao não comprometimento de sua operacionalização, inclusive quanto a uma suposta alternância de fornecedores, de executores de sua manutenção, de possível adoção de métodos variados de tecnologia empregados, isto é, fatores que possam interferir no perfeito funcionamento da Solução e causar sua descontinuidade operacional, o que pode significar perdas e danos irreparáveis à ANAC quanto aos dados processados e, consequentemente, aos serviços de TI prestados a seus públicos interno e externo.

1.6. As especificações técnicas da solução devem estar de acordo com o disposto neste Termo de Referência.

1.7. A solução visa atender necessidade de auditoria para todos os usuários internos da Agência que, atualmente, utilizam os serviços de diretório, correio eletrônico ou servidores de arquivos, num total de 2.400 colaboradores. Porém, a solução não se limita apenas às contas desses usuários, mas deve auditar todo tipo de conta de usuário ou de serviço ativo no ambiente de diretórios da Agência, assim como todo tipo de correio institucional existente no serviço de e-mail. Para o cálculo do quantitativo de licenças necessárias, foi considerado o quantitativo total de contas ativas atualmente relacionadas a cada colaborador da agência.

1.8. **Classificação dos bens e dos serviços comuns**

1.8.1. O objeto da licitação tem a natureza de bens e serviços comuns, nos termos do Decreto nº 10.024, de 20/09/2019, por ter padrões de desempenho e qualidade concisos e possíveis de serem definidos objetivamente, em perfeita conformidade com as especificações usuais praticadas no mercado.

2. JUSTIFICATIVA PARA O AGRUPAMENTO DOS ITENS

2.1. Embora a solução de TI seja composta por mais de um item, suas funcionalidades são unificadas e administradas em uma única interface de gerenciamento. Logo, a aquisição das soluções de auditoria, bem como a execução do suporte técnico e treinamento na forma identificada, garantem não só o melhor cumprimento dos requisitos de negócio, técnicos e tecnológicos, mas também uma melhor unicidade técnica para a entrega das funcionalidades requisitadas pela Agência. Além disso, o agrupamento dos itens permite uma gestão mais eficiente do ambiente de TI.

2.2. Alcance de maior eficiência não só no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico e o treinamento serão executados por um único fornecedor representante do fabricante. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

2.3. Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, conforme proposta na tabela do item 1.1 do tópico anterior.

2.4. Na situação em apreço, é imperativo destacar o que dispõe o Princípio da Padronização, insculpido no inciso I do art. 15 da Lei nº 8.666/1993, pelo qual se estabelece que a Administração, sempre que possível, tem o objetivo de compatibilizar especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia, segundo transcrição a seguir, *in verbis*:

> "Lei nº 8.666/1993
>
> Art. 15. As compras, sempre que possível, deverão:
>
> I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;
>
> (...);
>
> III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;"

2.5. Tal princípio, disposto no art. 15, Inciso I, da Lei 8666/1993, visa a propiciar à Administração uma consecução mais econômica e vantajosa de seus fins; e serve, pois, como instrumento de racionalização da atividade administrativa, por meio da redução de custos financeiros, tecnológicos, operacionais, gerenciais, técnico-administrativos e da otimização da aplicação de recursos. Isto é, fatores que se coadunam e se verificam na contratação ora pretendida. Significa, portanto, que, nesse caso, a padronização elimina variações tanto no tocante à seleção de equipamentos, componentes e produtos no momento da aquisição/contratação, como também na sua utilização, conservação, segurança e manutenção.

2.6. Dividir o objeto, nessa situação, ocasionará prejuízos técnicos, como também riscos de danos tecnológicos, visto que a manutenção, a garantia, o suporte técnico e o treinamento, se realizados por vários fornecedores, exigiriam um tempo excessivo em dirimir divergências entre possíveis incompatibilidades e causariam um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados ou divergentes.

2.7. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes da solução, melhor gerenciamento do contrato e obtenção dos serviços de suporte e treinamento padronizados.

2.8. Conforme Acórdão nº 861/2013 - TCU - Plenário -, é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação em tela, possui uma natural indivisibilidade, o que também inviabiliza a contratação de seus serviços por item de forma separada.

2.9. Segundo o Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". O lote proposto nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à competitividade.

2.10. O agrupamento também encontra amparo na jurisprudência do Tribunal de Contas da União, conforme se observa na Súmula 247 - TCU/2007.

> "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, **desde que não haja prejuízo para o conjunto ou complexo** ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade." (grifos nossos).

2.11. Em suma, a opção pelo fornecimento e consequente adjudicação por grupo leva em conta a modalidade de contratação pretendida e os benefícios associados. O agrupamento de vários itens num mesmo objeto não compromete a competitividade do certame, uma vez que várias empresas, que atuam no mercado, apresentam condições para cotar todos os itens.

3. DA JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. É extremamente necessário o uso de ferramentas e soluções adequadas que ofereçam segurança e eficiência a partir de um ambiente adequado à sua destinação. Segundo o instituto de pesquisas técnicas e análises de tendências de TI, o GARTNER GROUP, cerca de 80% dos dados estratégicos estão armazenados em base de dados não estruturadas ou semiestruturadas. Toda essa informação está distribuída em pastas (departamentais, setoriais e individuais) acessadas pelos diversos usuários da rede e gerenciadas por sistemas

operacionais que proporcionam registro de eventos (LOG'S) custoso e pouquíssimo informativo, que não proporcionam a devida granularidade para pesquisas de auditoria referente a quem, quando, onde e como um dado é utilizado.

3.2. Desta forma, quando são necessários o monitoramento de acesso aos dados armazenados, o gerenciamento e auditoria do repositório de usuários e e-mails, a execução de ações proativas em casos de incidentes de segurança cibernética e ataques de malware, ou até identificação de acessos indevidos de usuários internos mal intencionados, a equipe administradora da infraestrutura de TI fica refém da utilização de uma interface gráfica bastante ineficiente e que muitas vezes não é capaz de entregar as informações necessárias à análise, ficando o incidente sem as respostas necessárias e sem o devido tratamento.

3.3. Outro importante fator que deve ser mencionado diz respeito ao grande volume de informações que a auditoria nativa de nossa ferramenta de gestão de serviço de diretório, autenticação e gerenciamento de usuários armazena (AD - Microsoft). Como o volume de dados custodiados na infraestrutura mantida pela GEIT/STI é de difícil administração e muito extenso, a atividade de auditoria do ambiente é muito prejudicada e muitas vezes impossível de ser executada.

3.4. Além disso, o GARTNER GROUP apresentou também outro estudo que aponta que, em média, para cada 1 TeraByte de arquivos, existem 50.000 (cinquenta mil) pastas. Todas essas pastas armazenam arquivos com informações de cunho crítico ao funcionamento da instituição que são usadas no dia-a-dia por nossos usuários.

3.5. Todo esse grande volume de informações é gerenciado e utilizado por usuários que mudam frequentemente de cargo internamente. O problema é que essas mudanças muitas vezes não são informadas ou atualizadas no sistema onde as coletamos (SIGRH), e por consequência, os proprietários das pastas não são atualizados e elas ficam expostas a usuários que não deveriam mais ter acesso à informação. Isso acaba por comprometer estes dados, e infringir a Norma Complementar nº 20/IN01/DSIC/GSIPR, que estabelece "Diretrizes de Segurança da Informação e Comunicações (SIC) para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal, Direta e Indireta".

3.6. Fundamenta ainda essa necessidade, a IN nº 115 de 14 de Agosto de 2017, que instituiu a Política de Governança de Informações Digitais - PGID da ANAC, cujo objetivo é "estabelecer uma estrutura de governança de informações digitais, definindo competências e responsabilidades que nortearão as atividades de gestão de informações digitais da ANAC, para o atingimento dos princípios e diretrizes nela estabelecidos, bem como para assegurar que os ativos de informação digital provejam valor e sejam consistentes, íntegros e relevantes para subsidiar decisões dos públicos de interesse".

3.7. O exposto vai ao encontro das considerações do levantamento realizado pelo TCU no ano de 2008 que gerou o seguinte acórdão:

> "ACÓRDÃO Nº 1603/2008 - TCU – PLENÁRIO – Resultante do levantamento de Auditoria efetuado pela Secretaria de Fiscalização de Tecnologia da Informação – SEFTI, junto a Administração Pública Federal, com vistas a obter informações acerca da situação da gestão e do uso de Tecnologia da Informação – TI:
>
> ...
>
> 9.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR que oriente os órgãos/entidades da Administração Pública Federal sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso."

3.8. Reforça ainda a necessidade de execução dessa aquisição, as Seções II, III e VII da IN Nº 80/2014, da ANAC, que estabelece entre outras coisas a Proteção da Informação, a Gestão de Riscos, e o Controle de Acessos respectivamente, com a previsão de definição de níveis de proteção e controle durante o ciclo de vida da informação, contemplando manuseio, armazenamento, transporte e descarte, que estabelece a necessidade de gestão de riscos corporativos por meio de planejamento de segurança, fundamentado em desenvolvimento de cultura corporativa para riscos, qualificação de pessoas, desenvolvimento de procedimentos e implantação de tecnologias e recursos, e complementa que o acesso aos ativos de informação e sua utilização, quando autorizados, pode ser condicionado ao aceite a termo de sigilo e responsabilidade.

3.9. Um dos focos das fiscalizações de Tecnologia da Informação (TI), realizadas pela Secretaria de Fiscalização de Tecnologia da Informação (SEFTI), do Tribunal de Contas da União, é a verificação da conformidade e do desempenho das ações governamentais em aspectos de segurança de tecnologia da informação, utilizando critérios fundamentados. O principal objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão pública, para assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

3.10. A presente contratação tem por objetivo atender ainda demandas relacionadas à proteção destas informações, somada aos esforços já empregados nos anos anteriores e nos demais investimentos que estão em andamento no PDTI 2018/2019, e para esse atendimento temos como referência os padrões definidos na ABNT NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação.

> A NBR ISO/IEC 27002:2013, item 10.10, assim determina:
>
> "10.10 - Monitoramento"
>
> Objetivo: Detectar atividades não autorizadas de processamento de informação.
>
> Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados.
>
> Convém que registros (log) de operador e registros (log) de falhas sejam utilizados para assegurar que os problemas de sistemas de informação sejam identificados.
>
> Convém que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.
>
> Convém que o monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso."
>
> Ainda com relação à preservação dos logs, continua a referida norma técnica:
>
> "10.10.1 - Registros de auditoria
>
> Controle: Convém que registro (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.
>
> Diretrizes para implementação:
>
> Convém que os registros (log) de auditoria incluam, quando relevante:
>
> a) Identificação dos usuários;

b) Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (log-on) e saída (log-off) no sistema;

c) Identificação do terminal ou, quando possível, a sua localização;

d) Registro das tentativas de acesso ao sistema aceitas e rejeitadas;

e) Registros das tentativas de acesso a outros recursos e dados aceitos e rejeitados;

f) Alterações na configuração do sistema;

g) Uso de privilégios;

h) Uso de aplicações e utilitários do sistema;

i) Arquivos acessados e tipo de acesso;

j) Endereços e protocolos de rede;

k) Alarmes provocados pelo sistema de controle de acesso;

l) Ativação e desativação dos sistemas de proteção, tais como sistema de antivírus e sistema de detecção de intrusos."

Quanto ao monitoramento do uso do sistema (controle de acesso), a Norma recomenda:

"10.10.2 - Monitoramento do uso do sistema:

Controle: Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.

Controle: Convém que a organização esteja de acordo com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento. Convém que as seguintes áreas sejam consideradas;

a) Acessos autorizados, incluindo detalhes do tipo;

1. Identificador do usuário (ID de usuário);

2. A data e o horário dos eventos-chave;

3. Tipo do evento;

4. Os arquivos acessados;

5. Os programas ou utilitários utilizados;

b) Todas as operações privilegiadas, tais como:

1. Uso de contas privilegiadas, por exemplo: supervisor, root, administrador;

2. Inicialização e finalização do sistema;

3. A conexão e a desconexão de dispositivos de entrada e saída;

c) Tentativas de acesso não autorizadas, tais como:

1. Ações de usuários com falhas ou rejeitados;

2. Ações envolvendo dados ou outros recursos com falhas rejeitadas;

3. Violação de políticas de acesso e notificações para gateways de rede e firewalls, dentre outros."

E prossegue abordando a proteção e registro de logs:

"10.10.3 - Proteção das informações dos registros (logs):

Controle: Convém que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado.

Convém que os controle implementados objetivem a proteção contra modificações não autorizadas e problemas operacionais com os recursos dos registros (log). Registros de sistema precisam ser protegidos, pois os dados podem ser modificados e excluídos e suas ocorrências podem causar falsa impressão de segurança.

10.10.4 - Registros (log) de administrador e operador.

Controle: Convém que as atividades dos administradores e operadores do sistema sejam registradas.

Convém que esses registros (log) incluam:

a) A hora em que o evento ocorreu (sucesso ou falha);

b) Informações sobre o evento (exemplo: arquivos manuseados) ou falhas (exemplo: erros ocorridos e ações corretivas adotadas);

c) Que conta e que administrador ou operador estava envolvido;

d) Que processo estavam envolvidos."

3.11. Em recente análise do Processo de Gestão de Infraestrutura de TIC realizado pela Auditoria interna da Agência, constante no processo SEI nº 00058.518581/2017-22, foram identificados achados, relatados no Relatório de Auditoria nº 0898845, que corroboram para necessidade premente de execução deste projeto, especificamente, quanto aos assuntos abaixo relacionados:

a) Assunto 9: Deficiência nos procedimentos de segurança de redes

b) Assunto 11: Falha no processo de gestão da identidade

3.12. O volume de eventos diários é de mais de 1,5 milhões, com picos de até 2,5 milhões de eventos registrados nos computadores servidores de Administração do Domínio, correio eletrônico e servidores de arquivos, serviços esses utilizados pelos usuários da ANAC. Além disso, temos em nosso ambiente aproximadamente 7.617 grupos no AD, 10.676 objetos de usuários, sendo que 2.310 (21,6%) são usuários ativos, 1.985 (18,6%) são usuários inativos, 6.381 (59,8%) são usuários desabilitados, 1.904 (17,8%) são usuários com senhas que nunca expiram, e 816 (7,6%) são usuários com senhas expiradas. Ainda temos 8.511 contas de computador e 1.241 Unidades Organizacionais (OU).

3.13. Essa complexidade, volume e tamanho de usuários, contas, OUs (Unidades organizacionais), grupos, entre outros objetos, torna a gestão deste ambiente inexequível para os analistas e administradores da TI da GEIT/STI/ANAC, não sendo possível entregas com a qualidade necessária para atender às recomendações dos órgãos de controle da Administração Pública Federal (TCU e MPOG).

3.14. As atividades de auditar, controlar, gerenciar e monitorar as ações dos usuários, dos serviços de administração de diretório de usuários (Microsoft Active Directory), servidor de arquivos (Microsoft File Server) e correio eletrônico (Microsoft Exchange Server), bem como prevenir ações e comportamentos suspeitos em tempo real, proteger os dados sensíveis e gerir todas as permissões dos usuários de forma segura exigem soluções especializadas e eficientes que possibilitem automatizar essas tarefas.

3.14.0.1. São desafios que hoje esses analistas e administradores da TI enfrentam:

a) Identificar e classificar conteúdo sensível;

b) Identificar os proprietários dos dados;

c) Controle e auditoria de eventos (quem acessou o quê, e como acessou);

d) Excesso de demanda com falta de mão de obra para executar as tarefas;

e) Assegurar que as autorizações são baseadas em necessidades de negócios.

3.15. Assim, de acordo com os itens expostos, faz-se necessário a implementação de uma solução de auditoria, controle e governança para os diretórios de usuários (Microsoft Active Directory), os servidores de arquivos (Microsoft File Server) e o sistema de correio eletrônico (Microsoft Exchange Server), que realize monitoramento em tempo real e identifique desvios de comportamento dos usuários nestes repositórios.

3.16. Justifica-se, ainda, a execução deste projeto para eventual fornecimento de solução baseada em software, totalmente compatível com ambiente computacional da ANAC, para implantação de auditoria, controle e gerência de permissionamento dos repositórios de dados não estruturados residentes na infraestrutura interna da Agência.

3.17. Desta maneira, espera-se a adequação contínua das capacidades de controle e monitoramento necessárias aos serviços alocados no ambiente, aumentando o gerenciamento, eficiência e proteção das informações, simplificando tarefas complexas e permitindo uma fácil adaptação dos analistas e administradores da TI a alterações de emergência ou imprevistas. Permitindo, desta forma, o aumento na garantia de disponibilidade, confiabilidade, rapidez e segurança dos dados.

3.18. Esta contratação faz parte do Plano Diretor de Tecnologia da Informação - PDTI - 2018/2019 da ANAC, código PR18CP0048, cuja descrição é "implantar solução para gestão, monitoração, auditoria, automação e prevenção de perdas de dados no AD". A solução visa satisfazer necessidades corporativas e objetivos estratégicos da Instituição, cujo alinhamento é o demonstrado a seguir:

I - Planejamento Estratégico Institucional – PEI - 2015/2019:

a) Objetivo estratégico: 2.3 Garantir a efetividade da prestação de serviços de TI;

b) Estratégia: 2.3.1 Aprimorar o atendimento de demandas dos usuários da TI;

c) Iniciativa: 2.3.1.3 Otimizar o processo de atendimento a usuários de TI.

3.19. A contratação também está alinhada a objetivo estratégico da área de TI, conforme demonstrado abaixo:

I - Planejamento Estratégico de Tecnologia da Informação – PETI – 2016/2019:

a) Objetivo: 6 Aprimorar o atendimento de demandas dos usuários de TI;

b) Iniciativa: 6.3. Otimizar o processo de atendimento a usuários de TI da ANAC;

3.20. Conforme explicitado no Documento de Oficialização da Demanda – DOD, na seção "Metas do planejamento estratégico a serem alcançadas", “RESULTADOS A SEREM ALCANÇADOS”, são esperados os seguintes benefícios e resultados com essa contratação:

a) Aumentar o nível de atendimento e qualidade das operações de serviços de TI;

b) Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos;

c) Automação de controle de privilégios aos curadores dos dados e informações;

d) Classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos;

e) Análise comportamental dos usuários internos no ambiente computacional reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados;

f) Aprimorar a governança de TI;

g) Aprimorar governança de dados, informação e conhecimento;

h) Aprimorar a gestão de segurança da informação e comunicações;

i) Disponibilização de segurança e auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos e serviços de diretórios.

j) Garantir níveis satisfatórios de segurança da informação no âmbito da TI;

k) Garantir a efetividade da prestação de serviços de TI;

l) Criar e implementar plano de adequação de infraestrutura de TI;

m) Aprimorar a gestão da informação para a tomada de decisão;

n) Implantar um sistema de segurança da informação e comunicações;

o) Instituir o modelo de governança corporativa da ANAC;

p) Estruturar o processo de gestão corporativa de riscos;

q) Instituir sistema de gestão corporativa de riscos.

4. DAS ESPECIFICAÇÕES DOS REQUISITOS

4.1. DOS REQUISITOS DE NEGÓCIO

4.1.1. A presente contratação visa atender aos seguintes requisitos de negócio:

4.1.1.1. Aumentar o nível de atendimento e qualidade das operações de serviços de TI;

4.1.1.2. Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos;

4.1.1.3. Automatizar o controle de privilégios aos curadores dos dados e informações;

4.1.1.4. Classificar os dados armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos;

4.1.1.5. Analisar o comportamento dos usuários internos no ambiente computacional, reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados;

4.1.1.6. Aprimorar a governança de TI;

4.1.1.7. Aprimorar governança de dados, informações e conhecimentos;

4.1.1.8. Aprimorar a gestão de segurança da informação e comunicações;

4.1.1.9. Disponibilizar segurança, auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos, e de sistemas de TI;

4.1.1.10. Permitir pesquisas de auditoria referente a quem, quando, onde e como um dado é utilizado;

4.1.1.11. Monitoramento eficiente de acessos aos dados armazenados;

4.1.1.12. Gerenciamento e auditoria eficientes do repositório de usuários e e-mails;

4.1.1.13. Ações proativas em casos de incidentes de segurança cibernética e ataque de *malwares;*

4.1.1.14. Identificar acessos indevidos de usuários internos mal-intencionados;

4.1.1.15. Aproveitamento eficiente do espaço de armazenamento dos eventos de auditoria;

4.1.1.16. Atendimento dos princípios e diretrizes estabelecidos na IN 115/2017, que institui a Política de Governança de Informações Digitais - PGID da ANAC;

4.1.1.17. Implementação de parte dos pontos destacados nas seções II, III e VII, do Capítulo IV, da IN 080/2014, que institui a Política de Segurança da Informação e Comunicações - PoSIC no âmbito da Agência Nacional de Aviação Civil - ANAC;

4.1.1.18. Alinhamento a padrões definidos no item 10.10 da ABNT NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação;

4.1.1.19. Adequar a infraestrutura a achados da Auditoria interna do processo de gestão de infraestrutura de TIC (Documento SEI nº 0898845), relacionado a deficiência nos procedimentos de segurança de redes e falha no processo de gestão de identidades.

4.2. DOS REQUISITOS DE SEGURANÇA

4.2.1. A empresa a ser Contratada deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, assim como atender às normas e aos procedimentos de que trata a Instrução Normativa/ANAC nº 128, de 6 de novembro de 2018, relativos à Política de Segurança da Informação e Comunicações - PoSIC - no âmbito da Agência Nacional de Aviação Civil – ANAC, sem prejuízo dos demais atos, documentos e normativos expedidos e publicados pela Administração Pública Federal, bem como pela própria ANAC relativos ao sigilo, à segurança e à privacidade das informações e comunicações, além dos respectivos Termos de Compromisso e de Ciência previstos nas alíneas “a” e “b” do inciso V do art. 19 da Instrução Normativa/SLTI-MP nº 4, de 11 de setembro de 2014.

4.2.2. A contratada deverá credenciar seus profissionais junto à ANAC, caso seja necessário, para prestação de serviços e acesso às instalações da Sede da ANAC.

4.3. REQUISITOS DE IMPLANTAÇÃO

4.3.1. Os prazos e a sequência de eventos descritos na tabela abaixo devem ser obedecidos para a efetiva entrega, instalação e operacionalização da solução, e são requisitos essenciais para a emissão do Termo de Recebimento Definitivo (TRD):

EVENTO	DESCRIÇÃO	PRAZO	RESPONSÁVEL	PRAZO MÁXIMO
01	Início da Vigência do Contrato	-	ANAC e CONTRATADA	D
02	Reunião Inicial	Até 10 dias corridos após o evento 01.	ANAC e CONTRATADA	D+10
03	Emissão de ordem de fornecimento de bens e serviços e treinamento.	Até 10 dias corridos após o evento 02.	ANAC	D+20
04	Entrega do plano de instalação.	Até 10 dias corridos após o evento 03.	CONTRATADA	D+30
05	Avaliação, aprovação e solicitação de ajustes do Plano de Instalação	Até 07 dias corridos após o evento 04.	ANAC	D+37
06	Entrega da versão final do Plano de Instalação, com os ajustes solicitados pela ANAC	Até 07 dias corridos após o evento 05.	CONTRATADA	D+44
07	Entrega, instalação, configuração e operacionalização da solução.	Até 20 dias corridos após o evento 06.	CONTRATADA	D+64
08	Emissão do Termo de Recebimento Provisório (TRP) para os produtos e serviços (Itens 1 a 4)	Até 07 dias corridos após o evento 07.	ANAC	D+71
09	Emissão do Termo de Recebimento Definitivo (TRD)	Até 10 dias corridos após o evento 08.	ANAC	D+81

4.3.2. Dias corridos são aqueles ocorridos em quaisquer dias, úteis ou não.

4.3.3. O profissional responsável pelo plano de instalação e pela instalação, configuração e operacionalização da solução deve atender as requisitos descritos no item 11.3.2.

4.3.4. A empresa vencedora procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos da CONTRATANTE, sendo posteriormente aferido e testado o seu perfeito funcionamento.

4.3.5. A CONTRATADA deverá realizar a instalação de todos os componentes que compõem a solução no ambiente da ANAC, tomando-se por base o que foi definido nos itens da lista de requisitos, e sem nenhum ônus adicional para a contratante.

4.3.6. A CONTRATADA deverá realizar a configuração inicial de todos os componentes da solução no ambiente da ANAC, de forma a garantir que a solução será entregue à equipe técnica da ANAC em perfeitas condições de uso e monitoramento, considerando o atendimento de todos os requisitos descritos neste Termo de Referência, e sem nenhum ônus adicional para a contratante.

4.3.7. Os serviços de instalação das soluções abrangem as soluções descritas nos itens 1 a 4 da tabela de bens e serviços deste termo de referência.

4.4. DOS REQUISITOS TEMPORAIS

4.4.1. A CONTRATADA terá o prazo descrito no tópico anterior para instalação e configuração da solução no ambiente da contratante.

4.4.2. A CONTRATADA terá o prazo descrito no tópico 4.6.8 para atendimento e solução de chamados de garantia e suporte técnico.

4.4.3. A CONTRATADA terá o prazo descrito no tópico 4.6.9.14 para fornecimento do serviço de treinamento.

4.5. DOS REQUISITOS DE MANUTENÇÃO DO SOFTWARE E SUPORTE TÉCNICO

4.5.1. Os requisitos de manutenção do software, garantia e suporte técnico deverá ser atendido por um período de 36 (trinta e seis) meses, contados a partir da data de seu Aceite Definitivo (Evento 09 da tabela do item 4.3.1), e deve atender aos requisitos detalhados no item "Serviços de suporte técnico e garantia", tópico 4.6.8 deste Termo de Referência.

4.6. DOS REQUISITOS TÉCNICOS E FUNCIONAIS

4.6.1. Considerações Gerais

4.6.1.1. O não atendimento a qualquer um desses requisitos é fator impeditivo para a aceitação da proposta da licitante.

4.6.1.2. A solução deverá oferecer condições para gestão dos dados não estruturados de diretório de usuários, servidores de arquivos e serviço de e-mail, de forma que a equipe de TI da agência tenha condições de analisar, controlar e auditar os recursos e plataformas monitoradas.

4.6.1.3. A solução deverá fazer o monitoramento e auditoria dos usuários e seus acessos internos e externos ao diretório de usuários, pastas, arquivos e caixas de e-mail dos servidores monitorados.

4.6.1.4. O monitoramento e auditoria deverão gerar indicadores de performance para a gestão inteligente dos dados não estruturados, de forma que a agência possa evoluir e melhorar a performance, capacidade e segurança das informações e dos recursos monitorados.

4.6.1.5. Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo deverá ser executado de forma a diminuir o impacto sobre a disponibilidade dos serviços.

4.6.1.6. Devido à complexidade e à quantidade de servidores monitorados, todas as informações e plataformas monitoradas deverão ser apresentadas em uma única console integrada que atenda aos requisitos deste termo de referência e que deve ter seu acesso controlado por meio de autenticação baseada em usuários do domínio da agência.

4.6.1.7. Deve ser possível a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o acesso de analistas, equipe de suporte e usuários finais.

4.6.1.8. A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica.

4.6.1.9. Caso a solução seja compatível com sistemas operacionais Windows Server 2012 R2 ou superior ou distribuições linux gratuitas, não haverá necessidade do fornecimento de licenças.

4.6.1.10. A agência possui conhecimento e infraestrutura consolidada de banco de dados Microsoft SQL Server e Oracle. Portanto, a solução ofertada deverá reter as informações de log de acessos aos recursos monitorados em banco de dados Microsoft SQL Server ou Oracle. Nesse caso, não será necessário o fornecimento de licenças para o banco de dados.

I - Caso a solução fornecida seja incompatível com Microsoft SQL Server e Oracle, a contratada poderá utilizar outro sistema de banco de dados, desde que forneça todo o licenciamento do banco de dados necessário para a utilização da solução pela contratante. O licenciamento do banco de dados deve permitir seu uso pela solução de forma perpétua.

4.6.1.11. A solução deve permitir o acesso a, no mínimo, 10 anos de dados de auditoria capturados e armazenados.

4.6.1.12. A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização Microsoft Hyper-V.

4.6.1.13. Como a quantidade de servidores de arquivos, servidores de Exchange e controladores de domínio é variável, a solução deve ter escalabilidade para atender a quantidade crescente de servidores monitorados, sem a necessidade de aquisição de novas licenças.

4.6.1.14. Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação, como a ISO/IEC 27.001 ou similares.

4.6.1.15. As soluções fornecidas pela contratada devem contemplar a auditoria de sistemas na última versão disponibilizada pelo fabricante.

4.6.1.16. As soluções fornecidas devem permitir auditar, controlar, monitorar e gerenciar as contas de 2.400 colaboradores da Agência.

4.6.1.17. As soluções fornecidas devem permitir auditar, controlar, monitorar e gerenciar 3.200 contas ativas do domínio.

4.6.1.18. A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos, exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.

4.6.1.19. Deve ser possível, através da console, a criação de modelos de relatórios para posterior reutilização. Essa criação de modelos deve ser intuitiva e não deve necessitar da utilização de linguagem de programação ou outro software.

4.6.1.20. A documentação relativa às especificações técnicas da solução de TI deve ser fornecida em Português. Alternativamente, poderá ser apresentada em Língua Inglesa.

4.6.1.21. O licenciamento fornecido para todos os sistemas ou ferramentas que compõe essa solução deve ser perpétuo, não podendo, portanto, ter prazo de expiração de uso ou limitação de funcionalidades em função do tempo.

4.6.1.22. A solução deve permitir o acesso de, pelo menos, 10 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que são disponibilizadas a todos os usuários da agência, a solução deve permitir o acesso de todos os usuários.

4.6.1.23. A solução deve possuir interface nos idiomas Português ou Inglês.

4.6.1.24. Todos os itens apresentados nesta especificação são obrigatórios e deverão ser atendidos de forma nativa. Entende-se por itens atendidos de forma nativa, todos aqueles itens atendidos diretamente pelo software e seus módulos, sem a necessidade de alteração do código fonte em sua estrutura.

4.6.2. **Características Gerais – Permissões**

4.6.2.1. A solução deverá apresentar em sua interface todos os usuários e grupos de segurança dos diferentes domínios monitorados, assim como os usuários e grupos de segurança locais de cada servidor ou plataforma monitorada.

4.6.2.2. A solução deve permitir a busca por uma pasta nos servidores monitorados e apresentar quais usuários e grupos de segurança têm permissões e quais permissões esses objetos têm na pasta.

4.6.2.3. A solução deverá consolidar as permissões NTFS e *Share* de cada pasta e demonstrar a permissão efetiva dos usuários e grupos.

4.6.2.4. A solução deve utilizar os eventos coletados pela auditoria para realizar a análise comportamental automática dos usuários de maneira a fazer recomendações de revogação de acesso aos dados não estruturados dos servidores monitorados.

4.6.2.5. Além da visibilidade de permissões, usuários e grupos de segurança, deve ser possível realizar alterações de permissionamento dos usuários e grupos de segurança às pastas e diretórios dos servidores monitorados através da interface gráfica da solução.

4.6.2.6. A solução deve fornecer a visibilidade sobre aplicação de alterações e o histórico das alterações aplicadas através da console. Deve oferecer ainda a possibilidade de restaurar determinada alteração realizada.

4.6.3. **Características Gerais - Logs de auditoria dos recursos monitorados**

4.6.3.1. A solução deve coletar de forma automática e contínua logs de acessos a diretórios, pastas e arquivos dos servidores de arquivos monitorados, acessos a objetos do *Active Directory (AD)* e acessos a caixas postais do Exchange.

4.6.3.2. Deve ser possível, na interface gráfica da solução, visualizar os logs de auditoria de acessos a diretórios, pastas e arquivos dos servidores monitorados, acessos a objetos do AD e acessos a caixas postais do Exchange organizados e agrupados por recurso monitorado:

I - Pasta ou diretório: demonstrar todos os eventos para aquela pasta, subpastas e arquivos;

II - Unidade organizacional: demonstrar os eventos ocorridos em determinada OU;

III - Usuário ou grupo de segurança: demonstrar os eventos gerados ou sofridos por determinado usuário ou grupo.

4.6.3.3. Os eventos de auditoria coletados pela solução devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.

4.6.3.4. As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários, grupos de segurança e e-mails dos servidores monitorados.

4.6.3.5. Deve ser possível alterar também o conjunto de dados (colunas) retornados da consulta de auditoria de acordo com a necessidade da informação.

4.6.3.6. Todos os eventos dos diferentes servidores monitorados devem ser apresentados na mesma console gráfica da solução onde são também apresentadas as informações de permissionamento desses mesmos servidores monitorados.

4.6.3.7. A solução deve fornecer resumo das atividades auditadas, incluindo:

I - Quantidade de eventos por dia;

II - Visualização dos usuários mais e menos ativos nos servidores monitorados;

III - Visualização dos diretórios mais e menos acessados nos servidores monitorados;

IV - Visualização dos diretórios e pastas acessadas por um usuário ou grupo de segurança;

V - Visualização dos usuários inativos em uma pasta ou diretório.

4.6.4. **ITEM 1 - Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft *Active Directory).***

4.6.4.1. As funcionalidades descritas nas características gerais devem se aplicar à solução para os serviços de diretórios de usuários do *Microsoft Active Directory*, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados.

4.6.4.2. A solução descrita neste item deve possuir as seguintes funcionalidades globais:

I - Auditar ações sobre objetos do *Active Directory*;

II - Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;

III - Gerar alerta com base nas informações auditadas;

IV - Automatizar tarefas repetitivas, comum ou complexas;

V - Monitorar e analisar comportamentos suspeitos de usuários.

4.6.4.3. A solução deve oferecer a visibilidade gráfica da estrutura hierárquica de todos os domínios, OUs e objetos monitorados no AD da agência, apresentados na mesma console em que apresenta seus logs de auditoria.

4.6.4.4. A solução deve suportar a demonstração gráfica e a auditoria de diferentes domínios.

4.6.4.5. Deverá suportar as tecnologias DAS, SAN e suporte à tecnologia de cluster da Microsoft.

Funcionalidade: auditar ações sobre objetos do *Active Directory.*

4.6.4.6. A solução deverá fornecer informações detalhadas de auditoria para perícia em relação aos seguintes pontos:

I - Quem pode acessar e qual acesso pode fazer aos objetos do AD;

II - Quem faz alteração nos objetos;

III - Quem tem usado as credenciais para acessar os serviços de diretório;

IV - Detalhes dos eventos sobre objetos;

V - Quem possui permissões excessivas sobre os objetos;

VI - Quem deu ou revogou permissões de acesso e modificação.

4.6.4.7. A solução deverá ser capaz de rastrear quem fez alterações nos usuários, grupos, *OUs* e *GPOs* dos domínios monitorados do *Active Directory*, qual foi a alteração feita, quando foi feita, a máquina de origem da alteração e detalhes das propriedades tanto do objeto afetado quanto do objeto que gerou o evento.

4.6.4.8. A solução deverá indicar graficamente ou por relatório usuários ativos e inativos, usuários habilitados e desabilitados no AD.

4.6.4.9. A solução deve suportar a auditoria dos eventos do serviço de diretório, tais como:

I - Criação e deleção de todos os objetos;

II - Alteração de membros de grupos;

III - Alteração nas propriedades dos objetos do serviço de diretório;

IV - Requisições de acesso;

V - Autenticação de conta;

VI - Reconfiguração de senhas;

VII - Bloqueio e desbloqueio de conta;

VIII - Criação e deleção de conta;

IX - Habilitação e desativação de conta;

X - Eventos de permissão adicionada ou removida de objeto;

XI - Proprietário alterado;

4.6.4.10. A solução deve prover completa visibilidade sobre alterações em Objetos de Políticas de Grupos (GPO):

I - Modificação de configuração de GPOs;

II - Criação de link de GPO;

III - Deleção de link de GPO;

IV - Modificação de link de GPO.

Funcionalidade: gerar alerta com base nas informações auditadas e executar ações proativas, inclusive para múltiplos objetos do

***Active Directory*.**

4.6.4.11. A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado *syslog*, *eventlog*, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

4.6.4.12. A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

I - Atividades anômalas;

II - Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos;

III - Escalações de privilégios não autorizadas;

IV - Detecção de ferramentas de intrusão ou *malwares*.

4.6.4.13. O sistema de alerta em tempo real deve ser capaz de alarmar atividades em *Active Directory* (elevação de privilégios, inclusão/exclusão de grupos e usuários).

4.6.4.14. A solução deve permitir a integração com sistemas de e-mail padrão de mercado, inclusive Microsoft Exchange 2013, para envio de e-mails (alertas, notificações) de forma automática, ou manual.

Funcionalidade: monitorar e analisar os comportamentos suspeitos de usuários.

4.6.4.15. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

4.6.4.16. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.

4.6.4.17. Através da análise comportamental, solução deve realizar a descoberta automática de contas privilegiadas como usuários administrativos e contas de serviço.

4.6.4.18. Deve ser contemplada a assinatura de uma base de conhecimentos do fornecedor atualizada mensalmente de alertas pré-configurados de eventos suspeitos tais como:

I - Ataques de sequestro de dados (ransomware);

II - Detecção de ferramentas nocivas ao ambiente;

III - Excessos de ações com acessos negados;

IV - Acessos indevidos dos administradores nos dados da empresa;

V - Excessivas tentativas de elevação de privilégios;

VI - Excesso de tentativas de autenticação ou contas bloqueadas;

VII - Excesso de atividades em dados parados e/ou inativos;

VIII - Alterações excessivas e anormais em GPO;

IX - Excesso de acessos em caixas postais de uma única máquina;

X - Excesso de ações em um curto espaço de tempo.

4.6.4.19. A solução deve entregar painel web que permita análise dos comportamentos e eventos suspeitos listados.

4.6.4.20. Deve possuir um painel web interativo identificando ações tais como:

I - Quantidade de alertas e suas severidades em determinado período;

II - Usuários se comportando de forma suspeita;

III - Tipos de alertas mais disparados;

IV - Máquinas mais utilizadas para as ações suspeitas;

V - Servidores, pastas e mailboxes que mais sofrem ações suspeitas;

4.6.4.21. O painel deve mostrar as propriedades do usuário do AD essenciais para a perícia do alerta gerado.

4.6.4.22. Para análise do usuário mais alertado, o painel deve possuir página que agregue todos os alertas gerados por aquele usuário, permitindo que seja identificado o cenário do possível ataque.

4.6.4.23. No painel, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser personalizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.

4.6.4.24. A página com lista dos eventos deve apresentar gráfico que demonstre o quantitativo dos eventos em determinado período, para que seja possível identificar o desvio do comportamento indicado pela solução.

4.6.4.25. O painel deve fazer uma análise prévia dos alertas e correlacioná-los com outras informações e eventos do usuário alertado, dispositivo usado no momento do alerta, horário do evento.

4.6.4.26. Deve ser possível, a partir de selecionado evento alertado, fazer filtragem e correlacionamento com outros eventos como, por exemplo, o comportamento dos usuários do mesmo departamento do usuário alertado ou acessos ao mesmo tipo de informação sensível identificado pela solução.

4.6.4.27. O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Exchange) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tais como:

I - Quantidade de usuários habilitados inativos, usuários desabilitados, usuários habilitados com senhas expiradas, usuários habilitados bloqueados, grupos vazios, grupos não-administrativos com usuários administradores;

II - Número total de grupos de segurança, contas de usuários e computadores;

III - Quantidade de usuários com recomendação de revogação de permissão excessiva feita pela auditoria;

Funcionalidade: relatórios

4.6.4.28. A solução deve fornecer os seguintes relatórios:

I - Indicativos de uso de dados para a gestão de usuários, grupos de segurança e objetos do AD.

II - Logs de acessos e modificações de objetos do AD, com detalhamento dos eventos e metadados dos objetos afetados.

III - Todas as modificações de permissionamento de objetos dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de domínio.

IV - Alterações em grupos de segurança dos domínios monitorados.

V - Usuários inativos no domínio.

VI - Grupos de segurança vazios ou não utilizados.

VII - Usuários desabilitados que ainda fazem parte de grupos de segurança.

VIII - Histórico de membros de grupos de segurança.

IX - Estatísticas de autenticação e falha de autenticação.

X - Lista de usuários administradores em grupos não administrativos.

XI - Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental.

XII - Informações sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs dos domínios monitorados.

4.6.5. **ITEM 2 - Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de servidores de arquivos.**

4.6.5.1. As funcionalidades descritas nas características gerais devem se aplicar para as soluções anteriores, e também para a solução de servidores de arquivos Windows.

4.6.5.2. A solução descrita neste item deve possuir as seguintes funcionalidades globais:

I - Auditar acesso, modificação e remoção de pastas e arquivos em servidores de arquivos;

II - Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;

III - Gerar alerta com base nas informações auditadas;

IV - Automatizar tarefas repetitivas, comum ou complexas;

V - Permitir a delegação de gerenciamento de acessos aos proprietários dos dados;

VI - Monitorar e analisar comportamentos suspeitos de usuários.

4.6.5.3. A solução deve suportar como servidores de arquivos as versões do Windows Server 2008 ou versões superiores e Windows 7 e versões superiores.

4.6.5.4. A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios monitorados além de prever a possibilidade de criação de pastas e permissões para que a gestão do repositório seja centralizada.

4.6.5.5. A solução deve fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões.

4.6.5.6. A solução deve possuir compatibilidade comprovada no site do fabricante com storages EMC e HUAWEY, devendo possuir total compatibilidade com o ambiente da ANAC.

4.6.5.7. A interface gráfica da solução deverá permitir a busca por um usuário ou grupo de segurança e deverá apresentar suas permissões nas caixas postais e pastas dos servidores monitorados de forma integrada. As informações apresentadas incluem:

I - Identificação de herança de permissão ativada/desativada;

II - Indicação de existência de compartilhamento;

III - A fonte da permissão, ou seja, de que grupo o usuário está herdando a permissão.

Funcionalidade: permitir a delegação de gerenciamento de acessos aos proprietários dos dados.

4.6.5.8. A solução contratada deve oferecer um portal web integrado com os módulos de auditoria para que os proprietários das pastas tenham uma informação íntegra dos eventos de sua pasta.

4.6.5.9. A solução deverá permitir que os usuários donos das pastas concedam acesso às suas pastas ou grupos para outros usuários, bem como a revogação destes acessos, sem necessidade de envolvimento do administrador do sistema.

4.6.5.10. Deve fornecer método para assinalar ou associar um ou mais usuários como proprietário de uma pasta.

4.6.5.11. Uma vez realizada a requisição de nova credencial à pasta ou inclusão à um grupo, a solução ofertada deverá realizar as

configurações no ambiente sem que haja o envolvimento do administrador do sistema.

4.6.5.12. Deve ter interface web para solicitação de permissionamento ou participação em grupo de segurança e acesso à pasta.

4.6.5.13. Deve ser capaz de personalizar um fluxo de aprovação para cada demanda do usuário, permitindo dois ou mais aprovadores simultâneos ou em série.

4.6.5.14. A solução deverá ser capaz de enviar e-mail de notificação ao aprovador/dono da informação quando uma nova solicitação for aberta a ele.

4.6.5.15. O portal deve possibilitar a escolha de uma data de expiração ou validade do permissionamento aprovado, e realizar a revogação automática da permissão quando chegar a data de expiração sem que se faça necessária a intervenção de um usuário.

4.6.5.16. Deve suportar a revisão periódica de permissionamento.

4.6.5.17. Deve haver a recomendação das revisões de permissionamento de quais usuários poderiam ter suas permissões removidas sem que haja impacto ao negócio com base nas recomendações de uso e credenciais.

4.6.5.18. A solução ofertada deve disponibilizar para o responsável por cada conjunto de dados, acesso aos logs de auditoria, estatísticas e permissões.

4.6.5.19. Deverá permitir a criação de regras de segurança para que usuários ou grupos de usuários nunca tenham acesso a determinado conjunto de dados.

4.6.5.20. Deverá forçar as regras de segurança para que caso uma permissão seja concedida diretamente, o software as remova sem a intervenção de um usuário.

4.6.5.21. A solução deverá prover a habilidade de identificar os proprietários dos dados e enviar a eles relatórios sobre permissionamento e acesso.

4.6.5.22. O portal que fornece essa funcionalidade deve permitir o acesso de todos os colaboradores da Agência.

Funcionalidade: gerar alerta com base nas informações auditadas

4.6.5.23. A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado *syslog*, *eventlog*, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

4.6.5.24. A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

I - Atividades anômalas;

II - Acesso a dados sensíveis;

III - Arquivos sensíveis acessados ou excluídos;

IV - Escalações de privilégios não autorizadas;

V - Modificação de permissões em diretórios sensíveis;

VI - Detecção de ferramentas de intrusão ou *malwares*.

4.6.5.25. A solução de alerta em tempo real deve ser capaz de alarmar atividades em arquivos (deleção, abertura, movimentação, acessos negados, entre outras).

Funcionalidade: monitorar e analisar os comportamentos suspeitos de usuários

4.6.5.26. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

4.6.5.27. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.

4.6.5.28. A solução deve oferecer relatório dos alertas de comportamento anômalo identificados nos arquivos, pastas e diretórios dos servidores monitorados.

4.6.5.29. O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Exchange) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tais como:

I - Quantidade e tamanho total dos arquivos e pastas;

II - Dados sensíveis, parados e expostos;

III - Pastas com permissões inconsistentes, SIDs não resolvidos e usuários com ACEs diretas;

4.6.5.30. A solução deve atender todas as características comuns descritas nos itens 4.6.4.15 a 4.6.4.26.

Funcionalidade: relatórios

4.6.5.31. A solução deve fornecer os seguintes relatórios:

I - Indicativos de uso de dados para a gestão de arquivos e pastas.

II - Logs de acessos e modificações de arquivos e pastas, com detalhamento dos eventos e metadados dos objetos afetados.

III - Todas as modificações de permissionamento dos diretórios e pastas dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de arquivos.

IV - Pastas e diretórios dos servidores de arquivos monitorados onde há permissões concedidas a grupos de segurança globais (*Everyone, Users* ou *Authenticated Users*).

V - Pasta ou de todas as pastas do servidor que possuem SIDs não resolvidos.

VI - Pasta ou de todas as pastas do servidor que tenham permissão direta aplicada a usuários.

VII - Dados inativos ou sem utilização no domínio.

VIII - Histórico de permissões nas pastas e diretórios monitorados.

IX - Lista de pastas críticas com permissões excessivas nos servidores monitorados.

X - Lista de permissões em pastas dos servidores monitorados de usuários desabilitados.

XI - Pastas dos servidores monitorados sem permissões de administradores.

XII - Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental.

XIII - Estatística de acesso às pastas, utilização por tipo de arquivo, eventos por usuário e distribuição por tipos de evento sobre os servidores monitorados.

4.6.6. **ITEM 3 - Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de correio eletrônico (*Microsoft Exchange)*.**

4.6.6.1. As funcionalidades descritas nas características gerais devem se aplicar às caixas postais dos servidores de correio eletrônico Microsoft Exchange, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados não estruturados monitorados.

4.6.6.2. A solução descrita neste item deve possuir as seguintes funcionalidades globais:

I - Auditar acesso, modificação e remoção de caixas postais e listas do ambiente de correio eletrônico;

II - Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;

III - Gerar alerta com base nas informações auditadas;

IV - Monitorar e analisar comportamentos suspeitos de usuários;

V - Gerar relatórios sobre o ambiente de correio eletrônico.

4.6.6.3. A solução deve suportar as versões do Microsoft Exchange 2013 ou superior.

4.6.6.4. A solução deverá monitorar os eventos das caixas postais dos usuários do Exchange sem a necessidade de habilitação de auditoria nativa do Exchange (*journaling e diagnostics*);

Funcionalidade: auditar acesso, modificação e remoção de caixas postais e listas do ambiente de correio eletrônico.

4.6.6.5. A solução deverá coletar, de acordo com a versão monitorada, os seguintes eventos dos servidores de e-mail monitorados:

I - Pasta aberta;

II - Pasta criada;

III - Pasta deletada;

IV - Pasta renomeada;

V - Permissão adicionada a pasta;

VI - Permissão removida de pasta;

VII - Permissões de pastas alteradas;

VIII - Pasta movida;

IX - Pasta esvaziada;

X - Marcar todas como lidas;

XI - Mensagem aberta;

XII - Mensagem enviada;

XIII - Mensagem enviada “em nome de” (*on behalf of*);

XIV - Mensagem enviada “como” (“*As*”);

XV - Mensagem recebida;

XVI - Mensagem editada;

XVII - Mensagem deletada;

XVIII - Mensagem copiada;

XIX - Mensagem movida;

XX - Mensagem criada;

XXI - Mensagem marcada como não lida;

XXII - Mensagem marcada como lida;

XXIII - Informação de *logon*;

XXIV - Permissões adicionadas a *mailbox*;

XXV - Permissões removidas de mailbox;

XXVI - M*ailbox forward delivery option added*;

XXVII - *Mailbox forward delivery option removed.*

4.6.6.6. Respeitando a característica de cada protocolo, a solução deverá registrar os eventos com origem em diversos protocolos, tais como: POP3 – Post Office Protocol v3; IMAP4 – Internet Message Access Protocol; MAPI - Messaging Application Programming Interface; OWA – Outlook Web Access; EWS – Exchange Web Services; ActiveSync.

Funcionalidade: gerar alerta com base nas informações auditadas e executar ações proativas, inclusive para múltiplos objetos

4.6.6.7. A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitados para que seja disparado um e-mail, seja gerado *syslog*, *eventlog*, SNMP e que seja executado um script quando aquela ação específica ocorrer novamente.

4.6.6.8. A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

I - Atividades anômalas;

II - Acesso a dados sensíveis;

III - Detecção de ferramentas de intrusão ou malwares.

4.6.6.9. O sistema de alerta em tempo real deve ser capaz de alarmar atividades em exchange (leitura, movimentação, cópia e deleção de objetos – emails, eventos, entre outras atividades).

Funcionalidade: monitorar e analisar comportamentos suspeitos de usuários

4.6.6.10. A solução deve oferecer relatório dos alertas de comportamento anômalo identificados nas caixas postais dos servidores monitorados.

4.6.6.11. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

4.6.6.12. A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.

4.6.6.13. A solução deve atender também todas as características comuns descritas nos itens 4.6.4.15 a 4.6.4.26.

4.6.6.14. O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Exchange) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tal como:

I - Quantidade de mailboxes do Exchange.

Funcionalidade: relatórios

4.6.6.15. A solução deve fornecer os seguintes relatórios:

I - Indicativos de uso de dados para a gestão de caixas postais.

II - Logs de acessos e modificações de caixas postais, com detalhamento dos eventos e metadados dos objetos afetados.

III - Todas as modificações de permissionamento das caixas postais dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de correio.

IV - Estatística de acesso às caixas postais, eventos por usuário e distribuição por tipos de evento sobre os servidores monitorados.

4.6.7. **ITEM 4 - Licença perpétua de software de solução de tecnologia da informação para identificação e classificação de conteúdos sensíveis.**

4.6.7.1. A console de gerenciamento do módulo de classificação e identificação de informação sensível deve ser integrada à console de acesso às funcionalidades de permissionamento, visualização de logs a fim de fornecer maiores detalhes sobre as informações armazenadas no ambiente monitorado.

4.6.7.2. A solução deve inspecionar o conteúdo dos arquivos em escopo em busca de palavras, termos, expressões regulares, valores, e identificar informações sensíveis para o negócio.

4.6.7.3. A solução deve identificar dados sensíveis nas plataformas Windows.

4.6.7.4. A solução deve exibir na mesma interface gráfica as informações sobre os permissionamentos, ACL's , quantidade de informações sensíveis e qual tipo de informação sensível classificada, afim de facilitar a identificação de potenciais repositórios e pastas super expostos.

4.6.7.5. A solução deve gerar, em forma de relatórios, dados sobre a classificação das informações.

4.6.7.6. A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nas pesquisas dos logs.

4.6.7.7. A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nos relatórios de acesso.

4.6.7.8. Para cada arquivo marcado como sensível, a solução deve possibilitar a visão, diretamente da ferramenta, das expressões regulares ou caracteres que fizeram com que esse arquivo fosse considerado como sensível.

4.6.7.9. A solução deve fornecer visibilidade de conteúdo crítico de negócio através da classificação da informação.

4.6.7.10. A ferramenta deve fornecer visibilidade dos locais que possuem dados sensíveis.

4.6.7.11. A solução deve gerar recomendações acionáveis para redução de acesso aos dados classificados como sensíveis.

4.6.7.12. A solução deve integrar a funcionalidade de classificação de dados sensíveis com soluções de terceiros para estender a habilidade de ambos.

4.6.7.13. A solução deve possibilitar a instalação da funcionalidade de classificação de dados sensíveis nos mesmos servidores onde serão instaladas as funcionalidades de auditoria, sem a necessidade de servidores adicionais, diminuindo assim o esforço e custo da solução integrada.

4.6.7.14. A solução deve fornecer a funcionalidade de busca de arquivos através de palavras-chave, frases e/ou expressões regulares.

4.6.7.15. A ferramenta deve permitir integração com ferramentas de DLP (*Data Loss Prevention*) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução.

4.6.7.16. Deve ser possível definir o agendamento da classificação com hora de início e fim, frequência em que a busca ocorrerá e data em que deve parar, para que não haja impacto no ambiente.

4.6.7.17. A solução deve fornecer a funcionalidade de priorizar a busca por arquivos sensíveis para otimização da classificação. Pois desta forma, serão encontrados primeiro os arquivos nos locais mais relevantes.

4.6.8. **ITEM 5 - Serviços de suporte técnico e garantia**

4.6.8.1. Os serviços de suporte técnico e garantia abrangem:

I - Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

II - Elaboração de relatórios, estudos e diagnósticos sobre o ambiente monitorado;

III - Transferência de conhecimento aos técnicos da ANAC referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;

IV - Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

4.6.8.2. Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação.

4.6.8.3. Os serviços de suporte técnico e garantia de toda a solução deverão ser prestados por um período de 36 (trinta e seis) meses e deverão ser iniciados a partir da data Emissão do Termo de Recebimento Definitivo (TRD) da solução.

4.6.8.4. Os serviços de suporte técnico poderão ser prestados de forma remota ou presencial no endereço da CONTRATANTE, Setor Comercial Sul - Quadra 09 - Lote C - Edifício Parque Cidade Corporate - Torre A (1º ao 7º andar) Brasília - DF – CEP: 70.308-200.

I - O modelo de acesso remoto ao ambiente da ANAC será acordado com a CONTRATADA durante a vigência do contrato.

4.6.8.5. Os bens e produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas, independente da política de comercialização do fabricante.

4.6.8.6. Todas os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante.

4.6.8.7. A CONTRATADA deve disponibilizar profissional para aplicar as atualizações de versão e melhorias da solução no ambiente da ANAC pelo menos a cada 4 meses de contrato e quando efetivamente for necessário em função de atualização crítica para o funcionamento da solução, ou para alguma parametrização necessária para atender ao negócio, contados do Termo de Recebimento Definitivo (TRD), e durante todo o prazo de vigência do contrato.

4.6.8.8. A CONTRATADA deverá fornecer credencial de acesso à CONTRATANTE para os sistemas do fabricante que estejam relacionados a procedimentos de suporte e perguntas mais frequentes, caso seja disponibilizado este tipo de sistema por parte do fabricante e seja necessária credencial de acesso.

4.6.8.9. A CONTRATADA deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas.

4.6.8.10. A CONTRATADA deverá elaborar, a cada 4 meses, a partir do início do serviço de suporte técnico, relatório sobre a saúde do ambiente da CONTRATANTE utilizando informações fornecidas pela solução contratada. O relatório deve contemplar, no mínimo, as seguintes informações:

I - Saúde do ambiente de diretório;

II - Saúde do ambiente de correio;

III - Saúde do ambiente de servidores de arquivos;

IV - Análise de dados coletados para identificar e documentar áreas de risco e vulnerabilidades do ambiente;

V - Evolução em relação a informações de relatórios anteriores.

VI - Detalhamento de um plano de ação para correção dos problemas identificados, que será executado pela equipe interna da ANAC.

4.6.8.11. O relatório descrito no item anterior deverá ser confeccionado e finalizado durante mês em que se completa cada quadrimestre.

4.6.8.12. A CONTRATADA deverá disponibilizar para a CONTRATANTE uma central de atendimento (sítio na Internet, mensagem eletrônica e telefone) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, no mínimo, de 8hrs às 18hrs, em dias úteis.

I - Dias úteis são aqueles ocorridos entre segunda e sexta-feira, exceto feriados nacionais;

4.6.8.13. Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir um ticket do chamado técnico contendo, no mínimo:

I - Número do chamado;

II - Data e hora de abertura do chamado;

III - Previsão de conclusão do atendimento;

IV - Severidade do erro;

V - Descrição da solicitação.

4.6.8.14. A CONTRATADA deverá disponibilizar relatórios de chamados por período, contendo, no mínimo, as seguintes informações:

I - Número do chamado;

II - Data e hora de abertura do chamado;

III - Data e hora do início do tratamento do chamado;

IV - Data e hora de resolução do chamado;

V - Prazo Total de Início do Tratamento do Chamado (ITC);

VI - Prazo Total de Resolução do Chamado (PRC)

VII - Início do Tratamento do Chamado (ITC) cumprido (Sim/Não);

VIII - Prazo para Resolução do Chamado (PRC) cumprido (Sim/Não);

IX - Contato do técnico atendente;

X - Responsável pelo registro do chamado;

XI - Severidade do chamado;

XII - Descrição da solicitação;

XIII - Solução aplicada;

4.6.8.15. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da STI/ANAC e solicitará autorização para o fechamento deste. Caso a ANAC não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a ANAC fornecerá as pendências relativas ao chamado aberto.

4.6.8.16. A CONTRATANTE poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.

I - Estima-se o registro de uma quantidade maior de solicitações de suporte durante os primeiros 6 meses de contrato e a diminuição do quantitativo de solicitações nos meses seguintes.

4.6.8.17. A CONTRATADA deverá designar um profissional responsável pelo acompanhamento das solicitações de suporte abertas pela CONTRATANTE. Caberá a este profissional supervisionar os técnicos da CONTRATADA responsáveis pelo atendimento dos chamados abertos pela CONTRATANTE. Este profissional será o contato oficial da CONTRATANTE com a CONTRATADA para assuntos relativos aos serviços de suporte técnico. A comunicação da CONTRATANTE com esse profissional será realizada obrigatoriamente em português do Brasil;

4.6.8.18. A CONTRATADA deverá disponibilizar acesso para a CONTRATANTE ao sistema de abertura e fechamento de tickets para que seja possível extrair relatórios gerenciais de tickets.

4.6.8.19. Os prazos de solução dos chamados (Níveis Mínimos de Serviço) estão definidos a seguir, de acordo com a severidade do chamado:

Tabela de Severidade			
Severidade	**Descrição**	**Item do objeto do contrato**	**Prazo para Resolução do Chamado (PRC)**
Alta	Problemas graves que prejudicam a operação do produto ou limitação severa de suas funcionalidades com a paralisação parcial ou total da ferramenta.	Itens 1 a 4	Menor que 2 (dois) dias úteis a partir da abertura do chamado.
Média	Problemas que criam restrições à operação da solução, mas não comprometem seu uso e funcionamento.	Itens 1 a 4	Menor que 5 (cinco) dias úteis a partir da abertura do chamado.
Baixa	Aplicado em situações de esclarecimento de dúvidas ou suporte relacionadas à instalação, configuração e uso dos produtos adquiridos, bem como na atualização de versão de programa e/ou componente de software integrante da solução.	Itens 1 a 4	Menor que 8 (oito) dias úteis a partir da abertura do chamado.

4.6.8.20. Horas úteis são aquelas ocorridas em dias úteis, das 8 às 18hrs.

4.6.8.21. A contagem dos dias úteis para resolução do chamado se inicia no dia útil seguinte à abertura do chamado e se encerra às

18 horas do último dia do prazo.

4.6.8.22. O Prazo para Resolução do Chamado (PRC) será contabilizado a partir abertura da solicitação de assistência técnica pela CONTRATANTE.

4.6.8.23. O PRC poderá ser prorrogado em caso de defeitos que exijam a intervenção do laboratório do fabricante da solução, desde que aprovado pela CONTRATANTE, solicitado pela contratada antes do término do prazo e que a solução não esteja com problemas graves de operação.

4.6.8.24. A severidade do chamado será informada pela CONTRATANTE na ocasião da abertura da Ordem de Serviço.

4.6.8.25. O nível de severidade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra, não haverá o reinício de prazo.

4.6.8.26. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA para acompanhamento e controle da execução do serviço.

4.6.8.27. A CONTRATADA não poderá deixar de prestar assistência técnica sob a alegação de terem sido executadas anteriormente quaisquer tipos de intervenções (reparos/manutenções/atualizações) por parte da CONTRATANTE.

4.6.8.28. A frequência de aferição/ateste dos níveis de serviços será mensal, por meio da apresentação pela empresa a ser Contratada do Relatório de Acompanhamento de Execução do Contrato. A verificação dos indicadores também será realizada pela Equipe de Fiscalização do Contrato, devidamente designada pela ANAC, através da interface Web de relatórios, disponibilizada pela empresa contratada, ou por outro procedimento equivalente.

4.6.8.29. O relatório de Acompanhamento de Execução do Contrato, que deverá incluir o relatório de chamados para o período avaliado, deve ser entregue pela contratada até o dia 10 (dez) do mês subsequente.

4.6.8.30. O atraso injustificado na prestação dos "Serviços de suporte técnico e garantia", item V da tabela de bens e serviços, durante o período da garantia sujeitará a CONTRATADA a glosa, na forma a seguir:

I - Atraso na entrega do relatório quadrimestral, descrito no item 4.6.8.10, sobre a saúde do ambiente: 1,0% (um por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por dia útil de atraso, até o limite de 5 (cinco) dias úteis.

II - Não aplicação de atualizações a cada quadrimestre: 1,0% (um por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por dia útil de atraso, até o limite de 5 (cinco) dias úteis.

III - Atraso no prazo de entrega do relatório de Acompanhamento de Execução do Contrato: 1,0% (um por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por dia útil de atraso, até o limite de 5 (cinco) dias úteis.

IV - Atraso na solução do problema em relação ao prazo estipulado na Tabela de Severidade, referente aos chamados com **SEVERIDADE ALTA:** 2,5% (dois e meio por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por hora corrida de atraso, até o limite de 8 (oito) horas por chamado.

V - Atraso na solução do problema em relação ao prazo estipulado na Tabela de Severidade, referente aos chamados com **SEVERIDADE MÉDIA:** 1% (um por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por hora corrida de atraso, até o limite de 16 (dezesseis) horas por chamado.

VI - Atraso na solução do problema em relação ao prazo estipulado na Tabela de Severidade, referente aos chamados com **SEVERIDADE BAIXA:** 0,5% (meio por cento) do valor mensal do contrato do item "Serviços de suporte técnico e garantia", por hora corrida de atraso, até o limite de 24 (vinte e quatro) horas por chamado.

4.6.8.31. A glosa será calculada tomando por base os chamados fechados em um determinado mês, e considerará o somatório dos percentuais identificados nos incisos I a VI do item 4.6.8.30, limitado a 20% (vinte) do valor mensal do contrato do item "Suporte técnico e garantia".

4.6.8.32. Além das Glosas, os resultados das avaliações realizadas pela ANAC poderão resultar em sanções ou penalidades previstas na Lei nº 8.666/1993, caso a empresa Contratada não cumpra com os seus compromissos de qualidade e desempenho desejados.

4.6.8.33. A ocorrência de qualquer uma das glosas por 3 meses consecutivos poderá ensejar a aplicação de multa.

4.6.8.34. A condição para pagamento mensal pela ANAC é a execução dos serviços referente ao item "Serviços de suporte técnico e garantia" e a comprovação mediante apresentação, pela CONTRATADA, da seguinte documentação:

I - Nota Fiscal relativa aos serviços;

II - Relatório de Acompanhamento de Execução do Contrato;

III - Comprovação da instalação de atualizações, a cada quadrimestre;

IV - Aceitação pela contratada do relatório de saúde do ambiente, a cada quadrimestre.

4.6.9. **ITEM 6 - Treinamento para as soluções contratadas**

4.6.9.1. O treinamento será composto pelos módulos distintos que compõem a solução ofertada, que deve consistir na oferta de cursos presenciais ou remotos, e com abordagem prática voltada a todos os requisitos funcionais da solução.

I - Caso a CONTRATADA opte por treinamento presencial, ele deverá ser ministrado em Brasília/DF.

4.6.9.2. O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas para cada uma das quatro soluções contratadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

4.6.9.3. O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

4.6.9.4. A CONTRATADA será responsável pelos custos de elaboração, produção, impressão, fornecimento de ambiente virtual, e fornecimento de todo o material e logística necessários, bem como pela infraestrutura (salas, computadores, acesso à internet

e demais elementos necessários) e pelo transporte, acomodação, hospedagem, impostos, taxas, tributos, alimentação, diárias e passagens de seus colaboradores/instrutores para cumprimento das atividades necessárias à execução do treinamento e capacitação.

4.6.9.5. Toda a infraestrutura de transmissão remota do treinamento, caso essa seja a opção, será de responsabilidade da CONTRATADA.

4.6.9.6. A carga horária mínima exigida para este treinamento é de 28 horas.

4.6.9.7. A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 6 (seis) horas de instrução diária.

4.6.9.8. Deverá ser ministrada uma turma de treinamento que terá até 10 participantes.

4.6.9.9. Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento.

4.6.9.10. Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o local, o período de realização e o nome completo do participante.

4.6.9.11. O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

4.6.9.12. As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência do Contrato.

4.6.9.13. O público alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

4.6.9.14. Cronograma do Treinamento:

Evento	Descrição do evento	Prazo	Responsável	Prazo Máximo
1	Emissão da Ordem de Serviço de Treinamento	Até 10 dias corridos após o início da vigência do contrato.	ANAC	D+10
2	Entrega do Cronograma de Treinamento	Até 7 dias corridos após o evento 01.	CONTRATADA	D+17
3	Avaliação do Cronograma de Treinamento	Até 7 dias corridos após o evento 02.	ANAC	D+24
4	Ajustes no Cronograma de Treinamento	Até 7 dias corridos após o evento 03.	CONTRATADA	D+31
5	Execução dos Treinamentos	Até 30 dias corridos após o evento 04.	CONTRATADA	D+61
6	Entrega dos certificados, do manual dos treinamentos e da nota do treinamento	Até 7 dias corridos após o evento 05.	CONTRATADA	D+68
7	Emissão do Termo de Recebimento Provisório (TRP) do Treinamento	Até 7 dias corridos após o evento 06.	ANAC	D+75
8	Emissão do Termo de Recebimento Definitivo (TRD) do Treinamento	Até 10 dias corridos após o evento 07.	ANAC	D+85

4.6.9.15. A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a Agência.

4.6.9.16. A avaliação dos treinamentos deverá levar em consideração as questões listadas a seguir:

I - Avaliação do conteúdo:

a) Adequação dos conteúdos aos objetivos propostos;

b) Adequação das atividades desenvolvidas para alcance dos objetivos propostos;

c) Adequação do tempo para o alcance dos objetivos propostos;

d) Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;

e) Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;

f) Qualidade dos exemplos utilizados;

g) Aplicabilidade dos conhecimentos adquiridos no trabalho;

h) Contribuição para melhoria do desempenho no trabalho;

i) Qualidade do material instrucional (apostilas, gráficos etc.).

II - Avaliação do instrutor:

a) Formas/métodos de apresentação dos conteúdos;

b) Conhecimento dos temas tratados;

c) Visão prática dos conteúdos tratados;

d) Uso de estratégias para motivar os alunos em relação ao conteúdo;

e) Incentivo à participação dos alunos em sala de aula;

f) Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

III - Avaliação de ambiente e recursos (Treinamento presencial)

a) Qualidade do ambiente tecnológico destinado à realização do evento (geral);

b) Qualidade de iluminação;

c) Qualidade de ventilação;

d) Qualidade de acústica;

e) Recursos utilizados pelo instrutor (Quadro, projetor, bloco de cavalete - flipchart, tomadas, etc);

f) Qualidade do computador;

g) Qualidade do mobiliário (mesas, cadeiras, etc);

h) Facilidade de acesso ao local do treinamento;

i) Disponibilidade de estacionamento próximo;

IV - Avaliação de ambiente e recursos (Treinamento remoto)

a) Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração, etc);

b) Qualidade do ambiente virtual disponibilizado para o curso.

c) Qualidade da conexão disponibilizada pela contratada.

4.6.9.17. Em caso de treinamento presencial, a avaliação deverá considerar as questões listadas nos tópicos I, II e III do item 4.6.9.16.

4.6.9.18. Em caso de treinamento remoto, a avaliação deverá considerar as questões listadas nos tópicos I, II e IV do item 4.6.9.16.

4.6.9.19. Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

4.6.9.20. A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados pela ANAC.

4.6.9.21. O treinamento será considerado com qualidade suficiente, caso atinja uma nota igual ou superior a 8.

4.6.9.22. Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela contratada, juntamente com uma cópia dos formulários preenchidos pelos participantes.

4.6.9.23. Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da contratada, ela estará sujeita às sanções previstas no tópico 9.3 deste termo de referência.

5. DOS DEVERES E RESPONSABILIDADES DA CONTRATANTE

5.1. São obrigações da Contratante:

5.1.1. receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

5.1.2. verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo.

5.1.3. proporcionar todas as facilidades previstas e necessárias à perfeita execução do objeto deste Termo de Referência;

5.1.4. fiscalizar a execução do objeto deste Termo de Referência, sendo permitida a participação de terceiros para prestar assistência ou informações julgadas pertinentes;

5.1.5. exigir o cumprimento de todos os compromissos assumidos pela empresa contratada;

5.1.6. notificar, por escrito, a empresa contratada da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e à ampla defesa;

5.1.7. comunicar à contratada, por escrito, todas e quaisquer ocorrências relacionadas com o fornecimento da Solução de Tecnologia da Informação, para que seja substituído, reparado ou corrigido;

5.1.8. responsabilizar-se pelos pagamentos devidos, na forma pactuada no edital de licitação;

5.1.9. rejeitar, no todo ou em parte, os materiais e/ou serviços fornecidos em desacordo com as especificações constantes neste Termo de Referência;

5.1.10. fornecer à empresa contratada, em tempo hábil, as informações eventualmente necessárias à execução do objeto;

5.1.11. comunicar imediatamente à contratada quanto a defeitos ou irregularidades verificados na execução do objeto do Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente, para fins de correção ou readequação por parte da empresa;

5.1.12. aplicar as penalidades previstas para o caso de não cumprimento de cláusulas contratuais ou aceitar as justificativas apresentadas pela contratada;

5.1.13. vetar o emprego de qualquer produto, no todo ou em parte, que considerar incompatível com as especificações apresentadas na proposta da CONTRATADA, que possa ser inadequado, nocivo ou danificar seus bens patrimoniais ou ser prejudicial à saúde dos servidores.

5.1.14. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato, conforme o disposto no art. 30 da IN SLTI/MP 04/2014.

5.1.15. encaminhar formalmente a demanda por meio de Ordem de Serviço e/ou Fornecimento de Bens, de acordo com os critérios estabelecidos neste Termo de Referência, e de acordo com o modelo disponível no Anexo I - D deste Termo de Referência.

5.1.16. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.

5.1.17. Outras previstas na legislação pertinente.

5.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados

à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

6. DEVERES E RESPONSABILIDADES DA CONTRATADA

6.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

6.1.1. efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, versão e prazo de garantia;

6.1.2. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.1.3. substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

6.1.4. comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

6.1.5. manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

6.1.6. indicar formalmente preposto apto a representá-la durante a execução do contrato;

6.1.7. iniciar a execução do contrato nos prazos definidos contratualmente;

6.1.8. fornecer atualização tecnológica de todos os softwares e licenças entregues para a solução adquirida, a contar da data de aceite da implantação da solução e durante todo o período de vigência do contrato;

6.1.9. acatar as normas e diretrizes estabelecidas pela ANAC para execução do objeto deste Termo de Referência;

6.1.10. reutilizar, sempre que tecnicamente e tecnologicamente possível, as customizações, parametrizações e desenvolvimentos existentes no ambiente atual da ANAC;

6.1.11. submeter a prévia aprovação da ANAC toda e qualquer alteração na execução do objeto deste Termo de Referência;

6.1.12. sujeitar-se à fiscalização da ANAC, no tocante à execução deste objeto, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer;

6.1.13. comunicar ao Fiscal do Contrato ou a seu substituto, indicado pela ANAC, por escrito, qualquer anormalidade que ponha em risco a execução do objeto;

6.1.14. guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva da ANAC;

6.1.15. substituir imediatamente, a critério da ANAC, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado;

6.1.16. 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;

6.1.17. propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

6.1.18. encaminhar à ANAC todas as informações necessárias para viabilizar o recebimento e instalação das licenças;

6.1.19. promover o fornecimento dos materiais dentro dos parâmetros técnicos e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

6.1.20. prover os serviços de garantia e suporte técnico dentro dos prazos estabelecidos;

6.1.21. garantir que cada versão dos softwares funcionará substancialmente de acordo com a documentação para usuários, por todo o período de utilização da referida versão em qualquer computador da CONTRATANTE, obrigando-se a ressarcir inteiramente a ANAC de eventuais danos causados pela utilização do software, em função de erros ou bugs existentes no software;

6.1.22. entregar a documentação técnica completa e necessária em meio digital;

6.1.23. não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, da CONTRATANTE;

6.1.24. comunicar a ocorrência de incidentes de segurança e a existência de vulnerabilidades relativas ao objeto da contratação, em até 10 dias da sua ocorrência ou de ciência do incidente ou vulnerabilidade, assim como tomar as ações imediatas de contenção;

6.1.25. fornecer informações gerenciais sobre o desempenho dos serviços objeto do contrato, de maneira agregada e individualizada;

6.1.26. permitir a realização de auditoria em programas e equipamentos objeto do contrato pela contratante ou por instituição credenciada pelo Governo Federal;

6.1.27. apresentar os Termos de Ciência e de Compromisso na assinatura do contrato, conforme modelos apresentados nos anexos II e III deste Termo de Referência;

6.1.28. apresentar o Termo de Encerramento do Contrato;

6.1.29. atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual;

6.1.30. manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;

6.1.31. ceder os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração;

6.1.32. outras previstas na legislação pertinente.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. ROTINAS DE EXECUÇÃO

7.1.1. A CONTRATADA deverá indicar formalmente um preposto apto a representá-la junto à CONTRATANTE, o qual deve responder pela fiel execução dos serviços contratados, orientar os técnicos de manutenção que prestarão os serviços, bem como comparecer à contratante sempre que convocado. Para evitar que a contratante fique eventualmente sem acesso ao preposto, deverá ser indicado um substituto.

7.1.2. Em conformidade com o art. 30, da IN SLTI/MP Nº 04/2014, a CONTRATANTE deverá nomear, após a assinatura do contrato, Gestor e Fiscais Técnico, Administrativo e Requisitante para acompanhar e fiscalizar a sua execução.

7.1.3. Diante de situações de irregularidades de caráter urgente, o Preposto deverá comunicar-se, por escrito ou via e-mail, com a CONTRATANTE para apresentar os esclarecimentos julgados necessários, as informações sobre possíveis paralisações de serviços, a apresentação de relatório técnico, ou as razões justificadoras a serem apreciadas e decididas pelo agente designado.

7.1.4. As decisões e providências sugeridas pela CONTRATADA que forem julgadas imprescindíveis, mas que ultrapassarem a competência dos Fiscais designados pela ANAC, deverão ser encaminhadas à Gerência Técnica de Licitações e Contratos, para a adoção das medidas cabíveis.

7.2. DOS PRAZOS DE EXECUÇÃO

7.2.1. O fornecimento dos itens 1 a 4 da tabela de bens e serviços apresentada no item 1.1 deste Termo de Referência deverão seguir os prazos definidos no item 4.3.1 deste Termo de Referência.

7.2.2. A execução dos serviços do item 5 (Serviços de suporte técnico e garantia) da tabela de bens e serviços deste Termo de Referência será inicialmente prestado por um período de 36 (trinta e seis) meses e deverá ser iniciado a partir da data do Aceite Definitivo da solução de TI devidamente instalada, configurada e em produção no ambiente tecnológico da ANAC, conforme definidos no item 4.6.8 deste Termo de Referência.

7.2.3. A execução dos serviços do item 6 (Treinamento para as soluções contratadas) da tabela de bens e serviços deste Termo de Referência deverá seguir os prazos definidos no item "4.6.9.14. Cronograma do Treinamento", conforme descrito neste Termo de Referência.

7.3. DA SUBCONTRATAÇÃO

7.3.1. Não será permitida a subcontratação para o objeto deste certame.

7.4. DO PAGAMENTO

7.4.1. A nota fiscal/fatura deverá ser enviada à contratante, com a devida antecedência que permita o cumprimento dos prazos contratuais, sob pena de acréscimos dos dias de atraso aos respectivos prazos.

7.4.2. A nota fiscal/fatura só poderá ser emitida pela CONTRATADA após o aceite definitivo dos serviços associados ao contrato.

7.4.3. O pagamento ocorrerá após o ateste da nota fiscal/fatura pela equipe de fiscalização do contrato.

7.4.4. Os pagamentos serão realizados no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado, e conforme prazos e condições tabela a seguir.

7.4.4.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

Tabela de Pagamento			
Id	**Evento**	**Condição de Pagamento pela ANAC**	**Prazo para realização do Evento**
I	Entrega das licenças perpétuas e instalação de todos os componentes da solução no ambiente da ANAC (Itens 1 a 4).	Pagamento em parcela única, mediante Termo de Aceite Definitivo, após o ateste do recebimento das licenças e instalação de todos os componentes da solução no ambiente da ANAC e após recebimento da Nota Fiscal, conforme descrito nos "Requisitos de Implantação", item 4.3.	Até 30 (trinta) dias corridos, contados a partir do recebimento da Nota Fiscal ou Fatura.
II	Serviços de suporte técnico e garantia (Item 5)	Pagamento mensal do objeto contratado, mediante apresentação pela Contratada das seguintes informações: 1) Nota Fiscal relativa aos serviços; 2) Avaliação dos Níveis Mínimos de Serviços dos chamados registrados no suporte técnico; 3) Aplicação de atualizações de versão da solução autorizadas pela contratante, quando aplicável;	Até 30 (trinta) dias corridos da entrega da Nota Fiscal e comprovação de todas as condições necessárias para pagamento.

		3) Aprovação do relatório de saúde do ambiente, quando aplicável	
III	Treinamento para as soluções contratadas (Item 6)	Pagamento em parcela única, mediante Termo de Aceite Definitivo, após o treinamento ser ministrado e após comprovação de aprovação na avaliação do treinamento, conforme "Cronograma de Treinamento", conforme item 4.6.9.14.	Até 30 (trinta) dias corridos após a emissão do Termo de Aceite Definitivo do Treinamento.

7.4.5. O pagamento mensal dos serviços de suporte técnico e garantia equivale ao valor mensal contratado no item 5 da contratação.

7.4.6. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

7.4.7. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.4.7.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.4.8. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.4.8.1. o prazo de validade;

7.4.8.2. a data da emissão;

7.4.8.3. os dados do contrato e do órgão contratante;

7.4.8.4. o período de prestação dos serviços;

7.4.8.5. o valor a pagar; e

7.4.8.6. eventual destaque do valor de retenções tributárias cabíveis.

7.4.9. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

7.4.10. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

7.4.12. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

7.4.13. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.4.14. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.4.15. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

7.4.16. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

7.4.16.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

7.4.17. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.4.17.1. A Contratada 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.

7.4.18. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

7.4.19. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

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

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

7.5. **MECANISMOS FORMAIS DE COMUNICAÇÃO ENTRE A CONTRATADA E A ADMINISTRAÇÃO**

7.5.1. O representante da CONTRATADA deverá estar disponível em dias úteis, das 8h às 12h e das 14h às 18h.

7.5.2. O preposto deverá comparecer no ambiente do CONTRATANTE em até 12 (doze) horas úteis após convocação para participação em reunião.

7.5.3. A comunicação entre a ANAC e a CONTRATADA será realizada mediante contatos telefônicos com o preposto da contratada ou por meio de correio eletrônico em endereço a ser disponibilizado pela empresa contratada.

7.6. **TRANSFERÊNCIA DE CONHECIMENTO SOBRE A EXECUÇÃO E A MANUTENÇÃO DO OBJETO**

7.6.1. A instalação e configuração inicial de todos os componentes da solução deverão ser feitas com o acompanhamento de equipe técnica designada pela ANAC.

8. **MODELO DE GESTÃO DO CONTRATO**

8.1. **DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO**

8.1.1. As licenças da solução e o treinamento serão recebidos provisoriamente quando da entrega do objeto resultante de cada Ordem de Serviço ou de Fornecimento de Bens, pelo Fiscal Técnico do Contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

8.1.2. Uma vez emitido o Termo de Recebimento Provisório (TRP), iniciar-se-á a etapa de verificação.

8.1.3. Os bens e/ou serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes deste Termo de Referência e da proposta, devendo ser corrigidos, refeitos ou substituídos no prazo de 5 (cinco) dias, a contar da notificação da contratada, às custas da Contratada, sem prejuízo da aplicação de penalidades.

8.1.4. O Termo de Recebimento Definitivo (TRD) terá seu prazo final prorrogado pelo prazo utilizado para correção dos defeitos em caso de problemas no aceite da solução e do treinamento.

8.1.5. Os bens ou serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação de que os serviços prestados ou bens fornecidos atendem aos requisitos estabelecidos em contrato, com a consequente aceitação mediante termo circunstanciado.

8.1.5.1. O gestor do contrato analisará os relatórios e toda documentação apresentada pela fiscalização técnica e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.

8.1.5.2. O gestor emitirá Termo de Recebimento Definitivo dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato dimensionado pela fiscalização com base no Nível Mínimo de Serviço(NMS).

8.1.5.3. Na hipótese da verificação não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

8.1.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

8.2. **DA FISCALIZAÇÃO**

8.2.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, bem como do fornecimento das licenças e treinamento e instalação da solução, de forma a assegurar o perfeito cumprimento do contrato, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, consoante as disposições contidas na Instrução Normativa SLTI/MP nº 4, de 11 de setembro de 2014, e na forma dos Arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 10º do Decreto nº 9.507, de 2018 e de acordo com o Manual de Fiscalização de Contratos da ANAC.

8.2.2. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos produtos, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

8.2.3. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

8.2.4. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

8.2.5. A verificação da adequação da prestação do serviço, o fornecimento das licenças, a instalação da solução e o treinamento deverá ser realizada com base nos critérios previstos neste Termo de Referência.

8.2.6. A fiscalização técnica dos contratos avaliará constantemente a execução do objeto e utilizará o Nível Mínimo de Serviço (NMS), conforme previsto no Item 4.6.8, para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

8.2.6.1. não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida os serviços contratados; ou

8.2.6.2. deixar de utilizar recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8.2.7. Devem ser cumpridos os Níveis Mínimos de Serviço descritos neste Termo de Referência, que estabelecem requisitos para o suporte de produtos pela contratada.

8.2.8. Os indicadores de nível de serviço serão calculados com base nos chamados a serem faturados por período.

8.2.9. Sempre que houver quebra dos níveis de serviço aqui especificados, a CONTRATANTE poderá notificar a contratada, que terá prazo máximo de 5 (cinco) dias úteis para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação da contratada dentro desse prazo ou caso a contratante entenda serem improcedentes as justificativas, será iniciado processo de aplicação das sanções previstas.

8.2.10. A contratada deverá apresentar relatório que detalhe cada solicitação de suporte, conforme previsto no item 4.6.8.14 deste termo de referência.

8.2.11. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

8.2.12. O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

8.2.13. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

8.2.14. A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

8.2.15. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

8.2.16. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela Contratada ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 a 80 da Lei nº 8.666, de 1993.

8.3. DAS SANÇÕES ADMINISTRATIVAS

8.3.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

I - inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

II - ensejar o retardamento da execução do objeto;

III - falhar ou fraudar na execução do contrato;

IV - comportar-se de modo inidôneo; e

V - cometer fraude fiscal.

8.3.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

8.3.2.1. advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

8.3.2.2. multa de:

I - 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução e entrega dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

II - 0,1% (um décimo por cento) por dia até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumida;

III - 0,1% (um décimo por cento) por dia até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

IV - 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

V - 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

8.3.2.3. as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

8.3.2.4. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos.

8.3.2.5. impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

I - A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 12.1 deste Termo de Referência.

8.3.2.6. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

8.3.3. As sanções previstas nos subitens 8.3.2.1, 8.3.2.4, 8.3.2.5 e 8.3.2.6 poderão ser aplicadas à CONTRATADA juntamente com as de multa do subitem 8.3.2.2, descontando-a dos pagamentos a serem efetuados.

8.3.4. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor mensal do contrato
2	0,4% ao dia sobre o valor mensal do contrato
3	0,8% ao dia sobre o valor mensal do contrato
4	1,6% ao dia sobre o valor mensal do contrato
5	3,2% ao dia sobre o valor mensal do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
3	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	03
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
Para os itens a seguir, deixar de:		
5	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
6	Substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia;	01
7	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03
8	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01
9	Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA	01

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

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

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

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

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

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

8.3.8. As penalidades serão obrigatoriamente registradas no SICAF.

8.3.9. Sanções decorrentes da licitação serão dispostas no edital.

9. DOS VALORES ESTIMADOS

9.1. O valor global máximo a ser admitido por esta Agência para a presente contratação é de **R$ 7.495.064,00 (sete milhões, quatrocentos e noventa e cinco mil sessenta e quatro reais)**, devendo serem respeitados os valores máximos unitários e totais, conforme tabela abaixo:

GRUPO	Item	Descrição da solução	Unidade	Quantidade	Valor Unitário (R$)	Valor Total* (R$) para 3 anos
1	1	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft Active Directory).	Usuários	2.400	417,23	1.001.352,00
	2	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de servidores de arquivos.	Usuários	2.400	515,00	1.236.000,00
	3	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de correio eletrônico (Microsoft Exchange).	Usuários	2.400	538,40	1.292.160,00

	4	Licença perpétua de software de Solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis.	Usuários	2.400	456,30	1.095.120,00
	5	Serviços de suporte técnico e garantia	meses	36	78.512,00	2.826.432,00
	6	Treinamento para as soluções contratadas	turma	1	44.000,00	44.000,00
Valor Total (R$)						**7.495.064,00**

* valores a serem considerados para cadastramento e julgamento das propostas.

9.2. Além dos valores unitários e totais máximos para cada item, deverá ser respeitado o valor global máximo admitido para esta contratação.

9.3. A proposta de preços deverá vir acompanhada de documentação técnica que contenha a especificação clara e completa dos itens oferecidos, devendo conter o detalhamento de todas as suas características, sob pena de desclassificação.

9.4. No valor contratado estarão inclusas todas as despesas diretas e indiretas necessárias ao cumprimento integral do objeto contratado, não sendo permitida posterior inclusão.

9.5. Para os itens 1 a 4, o código SIASG Catser: 27464 – Licenciamento de direitos permanentes de uso de software para servidor.

9.6. Para o item 5, o código SIASG Catser: 27510 - Contratos de prestação de serviços de assistência técnica e científica.

9.7. Para o item 6, o Código SIASG Catser: 03840 – Treinamento - Sistema Informática / Software.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas com a execução dos serviços contratados correrão à conta dos recursos consignados à Agência Nacional de Aviação Civil – ANAC, no Orçamento Geral da União, para o exercício de 2019, conforme classificação orçamentária prevista no instrumento convocatório.

10.2. As despesas que ultrapassarem o presente exercício deverão correr à conta de orçamentos específicos, cujos créditos serão indicados oportunamente.

11. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1. Serão utilizados critérios correntes de mercado para a seleção do fornecedor.

11.2. Será exigido na proposta da licitante classificada em primeiro lugar da fase de lances, o cumprimento das seguintes cláusulas:

11.2.1. A proposta comercial da empresa a ser Contratada deverá demonstrar, explicitamente, que atende e contempla a totalidade das especificações técnicas previstas no item 4.6 deste Termo de Referência.

11.2.2. A proposta deve seguir o modelo apresentado no Anexo I - A deste Termo de Referência.

11.2.3. Deve-se fazer acompanhar à proposta, manuais, catálogos, folhetos, prospectos ou outros meios de divulgação do fabricante, disponíveis em links de URL'S públicos na Internet que sejam oficiais do fabricante, ou publicações originais que comprovem que a solução atende aos requisitos técnicos deste Edital.

11.2.4. Além de todos os documentos que comprovem os requisitos, deve-se fazer acompanhar à proposta o Anexo I - E - Tabela de cumprimento de requisitos -, preenchido com a identificação e página do documento onde se encontra descrito cada um dos requisitos da solução.

11.2.4.1. Os documentos entregues devem estar legíveis e serem pesquisáveis, para facilitar a análise da documentação.

11.2.5. Especificar de forma clara, completa e minuciosa, todos os itens ofertados;

11.2.6. Detalhar em suas propostas comerciais os preços unitários e total (anual e trienal) para cada um dos produtos licenciados, conforme modelo de proposta, disponibilizando planilha que tenha ao menos as seguintes informações:

11.2.6.1. Grupo

11.2.6.2. Item

11.2.6.3. Descrição da solução

11.2.6.4. Fabricante, especificação dos produtos e versão

11.2.6.5. Unidade

11.2.6.6. Quantidade

11.2.6.7. Valor unitário

11.2.6.8. Valor total anual por item e global

11.2.6.9. Valor total por item e global para os demais anos

11.2.6.10. Valor total por item e global trienal

11.2.7. Detalhar o valor total trienal global do contrato, considerado todo o período de vigência contratual.

11.2.8. Informar o prazo para entrega dos produtos, considerando o prazo máximo fixado neste Termo de Referência, contados a partir da assinatura do contrato.

11.2.9. Declaração expressa de que sua proposta engloba todas as despesas referentes ao fornecimento, bem como todos os tributos, encargos sociais e trabalhistas e quaisquer outras despesas que incidam ou venha a incidir sobre o objeto da licitação, bem como que possuem as condições necessárias para a execução dos serviços licitados.

11.2.10. A ANAC não assinará qualquer contrato com o fabricante para o recebimento das licenças decorrentes deste processo, ficando a LICITANTE obrigada a efetuar os seus pedidos cientes desta condição.

11.2.11. O processo de seleção do fornecedor será realizado por meio de procedimento licitatório na modalidade Pregão, na forma eletrônica, do tipo MENOR PREÇO, em sessão pública a ser realizada por meio do sistema eletrônico, no Portal de Compras Governamentais do Governo Federal, sítio http://www.comprasgovernamentais.gov.br/.

11.3. **Inspeções e Testes**

11.3.1. Para fins de verificação de adequação da solução ofertada às especificações técnicas detalhadas apresentadas no Edital:

11.3.1.1. A LICITANTE detentora do melhor lance poderá ser convocada pela CONTRATANTE para entregar e instalar a solução apresentada na proposta de preços no ambiente computacional da CONTRATANTE no prazo de até 2 dias úteis;

11.3.1.2. Findo o prazo de entrega e instalação da solução em todo o ambiente computacional da CONTRATANTE, será dado prazo de 5 (cinco) dias úteis para que a solução realize a coleta de dados/informações necessárias à posterior demonstração das funcionalidades exigidas da solução nos itens/subitens do Roteiro de Teste de Conformidade destacados diretamente dos REQUISITOS TÉCNICOS E FUNCIONAIS, item 4.6 deste Termo de Referência.

11.3.1.3. Findo o prazo determinado para coleta de dados/informações do ambiente pela solução ofertada, a LICITANTE deverá, no prazo de até 2 (dois) dias úteis, demonstrar à CONTRATANTE o atendimento pontual dos itens contidos no Roteiro de Teste de Conformidade destacados diretamente dos REQUISITOS TÉCNICOS E FUNCIONAIS item 4.6 deste Termo de Referência;

11.3.1.4. O software da solução a ser utilizado no teste não poderá ser diferente do apresentado na proposta de preço e também não poderá ser alterado ou customizado durante o período do teste, sob pena de reprovação.

11.3.1.5. No decorrer do teste, caso a solução ofertada pela LICITANTE não demonstre à equipe técnica da CONTRATANTE o atendimento de item constante no Roteiro de Teste de Conformidade o teste poderá ser finalizado para fins de economia processual e a solução ofertada será considerada reprovada;

11.3.1.6. Além dos representantes da LICITANTE responsável pela execução do teste sob supervisão da equipe técnica da CONTRATANTE, o teste poderá ser observado por somente 1 (um) representante das demais LICITANTES do certame, indicados por seus representantes via e-mail, com nome, cargo, CPF e declaração de vínculo com a empresa;

11.3.1.7. Durante o período do teste, os observadores somente poderão fazer considerações relativas ao teste por escrito e deverão direcioná-las à equipe técnica responsável pelo acompanhamento da CONTRATANTE. As considerações devem ser justificadas em conformidade com às especificações deste Termo de Referência e conforme o escopo do Roteiro de Teste de Conformidade, item 11.3.1.11 deste Termo de Referência;

11.3.1.8. Ao final do teste será lavrada a ata do teste a ser assinada pela equipe técnica da CONTRATANTE, pelos representantes da LICITANTE e os observadores, se houverem, com a indicação de atendimento ou não aos itens e a devida indicação de CLASSIFICAÇÃO ou DESCLASSIFICAÇÃO da LICITANTE;

11.3.1.9. A comprovação dos itens descritos no Roteiro de Teste de Conformidade não desobriga a LICITANTE de atender todos os outros itens previstos nos REQUISITOS TÉCNICOS E FUNCIONAIS do Termo de Referência deste Edital por meio da comprovação documental prevista no itens 11.2.3 e 11.2.4.

11.3.1.10. Caso a solução seja reprovada, a CONTRATANTE procederá com a convocação da próxima LICITANTE no certame em até 3 (três) dias úteis.

11.3.1.11. **Roteiro de Teste de Conformidade:**

I - Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação, como a ISO/IEC 27.001 ou similares.

II - A solução deve permitir a busca por uma pasta nos servidores monitorados e apresentar quais usuários e grupos de segurança têm permissões e quais permissões esses objetos têm na pasta.

III - Os eventos de auditoria coletados pela solução devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.

IV - As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários, grupos de segurança e e-mails dos servidores monitorados.

V - Deve ser possível alterar também o conjunto de dados (colunas) retornados da consulta de auditoria de acordo com a necessidade da informação.

VI - A solução deve oferecer a visibilidade gráfica da estrutura hierárquica de todos os domínios, OUs e objetos monitorados no AD da agência apresentados na mesma console em que apresenta seus logs de auditoria.

VII - A solução deve suportar a auditoria dos eventos do serviço de diretório, tais como:

a) Criação e deleção de todos os objetos;

b) Alteração de membros de grupos;

c) Alteração nas propriedades dos objetos do serviço de diretório;

d) Requisições de acesso;

e) Autenticação de conta;

f) Reconfiguração de senhas;

g) Bloqueio e desbloqueio de conta;

h) Criação e deleção de conta;

i) Habilitação e desativação de conta;

j) Eventos de permissão adicionada ou removida de objeto;

k) Proprietário alterado;

l) Modificação de configuração de GPOs;

m) Criação de link de GPO;

n) Deleção de link de GPO;

o) Modificação de link de GPO.

VIII - A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado *syslog*, *eventlog*, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

IX - A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

a) Atividades anômalas;

b) Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos;

c) Escalações de privilégios não autorizadas;

d) Detecção de ferramentas de intrusão ou *malwares*.

X - A solução deverá permitir que os usuários donos das pastas concedam acesso às suas pastas ou grupos para outros usuários, bem como a revogação destes acessos, sem necessidade de envolvimento do administrador do sistema.

XI - Através da análise comportamental, solução deve realizar a descoberta automática de contas privilegiadas como usuários administrativos e contas de serviço.

XII - Para análise do usuário mais alertado, o painel deve possuir página que agregue todos os alertas gerados por aquele usuário, permitindo que seja identificado o cenário do possível ataque.

XIII - A solução deve fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões.

XIV - A solução deve fornecer os seguintes relatórios:

a) Indicativos de uso de dados para a gestão de arquivos e pastas.

b) Logs de acessos e modificações de arquivos e pastas, com detalhamento dos eventos e metadados dos objetos afetados.

c) Todas as modificações de permissionamento dos diretórios e pastas dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de arquivos.

d) Pastas e diretórios dos servidores de arquivos monitorados onde há permissões concedidas a grupos de segurança globais (Everyone, Users ou Authenticated Users).

e) Pasta ou de todas as pastas do servidor que possuem SIDs não resolvidos.

f) Pasta ou de todas as pastas do servidor que tenham permissão direta aplicada a usuários.

g) Lista de pastas críticas com permissões excessivas nos servidores monitorados.

h) Lista de permissões em pastas dos servidores monitorados de usuários desabilitados.

i) Pastas dos servidores monitorados sem permissões de administradores.

j) Estatística de acesso às pastas, utilização por tipo de arquivo, eventos por usuário e distribuição por tipos de evento sobre os servidores monitorados.

XV - A solução deverá monitorar os eventos das caixas postais dos usuários do Exchange sem a necessidade de habilitação da auditoria nativa do Exchange (*journaling e diagnostics*);

XVI - A solução deverá coletar, de acordo com a versão monitorada, os seguintes eventos dos servidores de email monitorados:

a) Pasta aberta;

b) Pasta criada;

c) Pasta deletada;

d) Pasta renomeada;

e) Permissão adicionada a pasta;

f) Permissão removida de pasta;

g) Permissões de pastas alteradas;

h) Pasta movida;

i) Pasta esvaziada;

j) Marcar todas como lidas;

k) Mensagem aberta;

l) Mensagem enviada;

m) Mensagem enviada “em nome de” (on behalf of);

n) Mensagem enviada “como” (“As”);

o) Mensagem recebida;

p) Mensagem editada;

q) Mensagem deletada;

r) Mensagem copiada;

s) Mensagem movida;

t) Mensagem criada;

u) Mensagem marcada como não lida;

v) Mensagem marcada como lida;

w) Informação de *logon*;

x) Permissões adicionadas a *mailbox*;

y) Permissões removidas de *mailbox*;

XVII - A solução deve fornecer os seguintes relatórios:

a) Indicativos de uso de dados para a gestão de caixas postais.

b) Logs de acessos e modificações de caixas postais, com detalhamento dos eventos e metadados dos objetos afetados.

c) Todas as modificações de permissionamento das caixas postais dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de correio.

XVIII - A console de gerenciamento do módulo de classificação e identificação de informação sensível deve ser integrada à console de acesso às funcionalidades de permissionamento, visualização de logs a fim de fornecer maiores detalhes sobre as informações armazenadas no ambiente monitorado.

XIX - A solução deve inspecionar o conteúdo dos arquivos em escopo em busca de palavras, termos, expressões regulares e valores e identificar informações sensíveis para o negócio.

XX - A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nas pesquisas dos logs.

XXI - A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nos relatórios de acesso.

XXII - Para cada arquivo marcado como sensível, a solução deve possibilitar a visão, diretamente da ferramenta, das expressões regulares ou caracteres que fizeram com que esse arquivo fosse considerado como sensível.

XXIII - A solução deve fornecer visibilidade de conteúdo crítico de negócio através da classificação da informação.

11.4. **Da Qualificação Técnica**

11.4.1. A licitante ou interessada deverá apresentar Atestado de Capacidade Técnica em seu nome, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove ter prestado serviços de entrega, instalação, configuração e apoio técnico para solução de auditoria e outras funcionalidades em ambiente computacional de servidores de arquivos, diretórios de usuários e correio eletrônico. O Atestado deve considerar os seguintes requisitos:

11.4.1.1. que o número mínimo de usuários fixos da instituição fornecedora do referido Atestado seja da ordem de 1.000 (mil);

11.4.1.2. No atestado de Capacidade Técnica a ser apresentado pela licitante/interessada, deve estar explícito:

I - A organização que o está fornecendo;

II - O responsável pelo Setor/Unidade encarregado(a) do objeto em questão;

III - Os contatos da organização que forneceu o atestado, para fins de realização de diligência;

IV - A especificação dos bens fornecidos, bem como os serviços executados ou em execução.

11.4.1.3. O atestado de capacidade técnica, documentações e comprovações necessárias para que a administração comprove a veracidade das informações deverão conferir com o CNPJ da empresa licitante;

11.4.1.4. Não será aceito somatório de atestados de capacidade técnica para comprovação do número mínimo de usuários fíxos.

11.4.1.5. JUSTIFICATIVA DA RELEVÂNCIA TÉCNICA: a exigência da apresentação dos Atestado(s) de Capacidade Técnica tem por objetivo avaliar a experiência e a habilidade técnica da licitante ou interessada na execução dos serviços, como também no fornecimento dos bens relativos à contratação, objeto da presente licitação, tanto em características quanto em quantidades. Destaca-se que os quantitativos aqui solicitados refletem o mínimo necessário considerado pela ANAC, para atendimento aos Serviços de TI prestados pela Agência, que, atualmente, conta com um quantitativo de cerca de 2.400 (dois mil e quatrocentos) colaboradores.

11.5. No momento da assinatura do contrato, a adjudicatária deverá apresentar declaração, datada e assinada por seu representante legal, de que disporá de profissional com nível superior e com as seguintes certificações ou equivalentes:

11.5.1. No mínimo 01 (um) técnico profissional capacitado e certificado na linha de produtos proposta;

11.5.2. Caso o fabricante não possua certificação específica para a linha de produtos serão aceitos profissionais comprovadamente capacitados e aprovados em treinamento formal do fabricante.

12. **DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL**

12.1. Não são aplicáveis a essa contratação por se tratar de aquisição de solução de software e prestação de serviços de suporte técnico, sem fornecimento de equipamentos, componentes ou peças e também sem gerar impacto direto ao meio ambiente.

13. DOS DIREITOS DE PROPRIEDADE INTELECTUAL

13.1. Fica a empresa a ser contratada obrigada a guardar inteiro sigilo dos dados processados, reconhecendo que esses dados são de propriedade exclusiva da ANAC, e que são vedados a cessão, a locação, o uso ou a venda deles a terceiros sem prévia autorização formal da ANAC.

13.2. A empresa a ser contratada deverá entregar à ANAC toda e qualquer documentação produzida decorrente da execução do objeto dessa contratação, bem como deverá ceder à ANAC, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos estudos, relatórios, divulgações em mídias físicas ou virtuais, em páginas da intranet, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, demais resultados afins produzidos e obtidos, durante a vigência do Contrato a ser firmado e de eventuais e pertinentes Termos Aditivos.

13.3. Ficam reservados à ANAC os direitos de propriedade intelectual e direitos autorais da Solução de TI relativos aos diversos produtos e documentos produzidos ao longo do Contrato a ser firmado, incluindo-se a documentação, os modelos de dados e as bases de dados, restando, portanto, a obrigação de serem devidamente justificados os casos em que tais direitos não vierem a pertencer à Agência.

13.4. As informações sob custódia do fornecedor serão tratadas como informações sigilosas, não podendo ser usadas por este fornecedor ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do contratante.

14. DO REAJUSTE DO CONTRATO

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

14.1.1. Dentro do prazo de vigência do contrato, mediante solicitação da contratada e após o interregno de um ano, exclusivamente para o **item 5** relativo aos **serviços de suporte técnico e garantia,** os preços contratados poderão sofrer reajuste, aplicando-se o índice descrito no item 14.5 exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

14.2. O interregno mínimo de 1 (um) ano para o 1º (primeiro) reajuste de que trata o item antecedente será contado a partir da data limite para apresentação de propostas constante do instrumento convocatório, ou do orçamento a que a proposta se referir, em relação aos custos dos serviços de suporte técnico e garantia dispostos e/ou previstos na pertinente Proposta Comercial da Contratada.

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

14.4. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

14.5. O reajuste de que trata esta cláusula será efetuado com base no Índice de Custos de Tecnologia da Informação – ICTI, calculado e divulgado pelo Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, ou outro índice que venha a substituí-lo por força de determinação legal ou por sua falta ou descontinuidade.

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

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

14.8. 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.

14.9. O reajuste será realizado por apostilamento.

14.10. Quando da solicitação do reajuste de que trata esta Cláusula, este somente será concedido mediante a comprovação pela Contratada do aumento dos custos ali especificados, considerando-se:

14.10.1. a apresentação de nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo que retrata a variação dos custos específicos;

14.10.2. o adequado índice de que trata esta Cláusula, o qual retrate a variação dos preços relativos aos custos objeto do pretenso reajuste, desde que devidamente individualizados na mencionada Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo da Contratada;

14.10.3. a disponibilidade financeira e orçamentária do órgão ou entidade Contratante.

14.11. É vedada a inclusão na nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo previstos no item antecedente, por ocasião da solicitação do reajuste de que trata esta Cláusula, de materiais, equipamentos, componentes, peças, acessórios, produtos não previstos na originária Proposta Comercial da Contratada, exceto quando se tratar das situações e casos devidamente comprovados e acompanhados da respectiva justificativa e documentação comprobatória atestada pela procedente Equipe Técnica responsável pela pertinente Gestão e Fiscalização Contratual.

14.12. Não sendo juntada à solicitação de reajuste de que trata esta Cláusula a mencionada nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo que retrata a variação dos custos específicos, o adequado índice de que trata esta mesma Cláusula, juntamente com a pertinente documentação comprobatória, a análise pela parte da Contratante ficará suspensa até a apresentação da devida documentação.

15. DA GARANTIA DA EXECUÇÃO

15.1. O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

15.2. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contados da assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

15.2.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

15.2.2. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.

15.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

15.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

15.4.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

15.4.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

15.4.3. multas moratórias e punitivas aplicadas pela Administração à contratada; e

15.4.4. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

15.5. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

15.6. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

15.7. 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 Fazenda.

15.8. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

15.9. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

15.10. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de ..10.... (DEZ) dias úteis, contados da data em que for notificada.

15.11. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

15.12. Será considerada extinta a garantia:

15.12.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

15.12.2. no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2"do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

15.13. O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

15.14. A contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

16. DA ALTERAÇÃO SUBJETIVA

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

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	**Integrante Requisitante**	**Integrante Administrativo**
Marcelo Augusto Curado Fleury Teixeira **Matrícula:** 2030374	Marcelo Nogueira Lino **Matrícula:** 2126657	Aderson de Lima Calazans **Matrícula:** 1526378

ANEXO I - A - MODELO DE PROPOSTA DE PREÇO

À

AGENCIA NACIONAL DE AVIAÇÃO CIVIL (ANAC)

PREGÃO Nº ___/2019

SESSÃO PÚBLICA: ___/___/2019

HORÁRIO: ___ HORAS

Proposta que faz a empresa _____.

GRUPO	Item	Descrição da solução	Fabricante, especificação dos produtos e versão	Unidade	Quantidade	Valor Unitário (R$)	Valor total - ANO 1 (R$)	Valor Total - Demais anos (R$)	Valor Total* (R$) (3 anos)
1	1	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft *Active Directory).*		Usuários	2.400				
	2	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de servidores de arquivos.		Usuários	2.400				
	3	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de correio eletrônico (*Microsoft Exchange).*		Usuários	2.400				
	4	Solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis, com licença perpétua.		Usuários	2.400				
	5	Serviços de suporte técnico e garantia		meses	36				
	6	Treinamento para as soluções contratadas		turma	1				
						Valor Total (R$)			

* Adequar aos valores finais ofertados na proposta comercial.

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 ___/2019-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 garantia, 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:**			
Banco:		**Agência:**		**Conta Corrente:**	

Dados do Representante para fim de apresentação da proposta e assinatura do contrato:

Nome:			
CPF:		**Cargo/Função:**	
Carteira de identidade:		**Expedido por:**	
Nacionalidade		**Estado Civil**	
Endereço:			
Telefone:		**Fax:**	
Endereço eletrônico:			

Em anexo a essa proposta, seguem os documentos exigidos no item 11 do Termo de Referência.

Local e data

_____

Assinatura e carimbo
(Representante Legal)

ANEXO I- B - TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

INTRODUÇÃO

Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato No.:			
Objeto:			
Contratante:			
Gestor do Contrato:		**Matrícula:**	
Contratada:		**CNPJ:**	
Preposto da Contratada:		**CPF:**	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

_____

Nome:

Matrícula:

_____

Nome:

Matrícula:

ANEXO I- C- TERMO DE COMPROMISSO

TERMO DE COMPROMISSO

O ***<Nome do Órgão>***, sediado em ***<Endereço>***, CNPJ n° ***<CNPJ>***, doravante denominado CONTRATANTE, e, de outro lado, a ***<Nome da Empresa>***, sediada em ***<Endereço>***, CNPJ n° ***<CNPJ>***, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX 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 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:

CLÁUSULA PRIMEIRA – DO 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, 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 maio de 2011, 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.

CLÁUSULA SEGUNDA – DOS 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.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

CLÁUSULA TERCEIRA – 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;

CLÁUSULA QUARTA – 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.

CLÁUSULA QUINTA – DOS 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 expresso e prévio 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, mesmo 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.

CLÁUSULA SEXTA – DA 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.

CLÁUSULA SÉTIMA – DAS 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 Art. 87 da Lei nº. 8.666/93.

CLÁUSULA OITAVA – 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 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 a 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.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da , 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.

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.

DE ACORDO

CONTRATANTE	CONTRATADA
_____ Nome: Matrícula:	_____ Nome: Matrícula:
Testemunha 1 _____ Nome: Qualificação:	Testemunha 2 _____ Nome: Qualificação:

ANEXO I - D - MODELO DE ORDEM DE SERVIÇO E/OU FORNECIMENTO DE BENS

ORDEM DE SERVIÇO E/OU FORNECIMENTO DE BENS

Por intermédio desta orde de serviço e/ou fornecimento de bens solicita-se, formalmente à Contratada, a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato.

IDENTIFICAÇÃO					
Contrato nº					
Contratada					
Contratante	Agência Nacional de Aviação Civil (ANAC)				
Ordem de Serviço Nº	XXX/ANO	**Data de emissão**			
Solução de TI		**Fase da execução**			
INFORMAÇÕES DO SOLICITANTE					
Usuário Solicitante		**E-mail do solicitante**			
Área		**Telefone**			
ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO					
Item	**Descrição do produto**	**Métrica (unidade/mês)**	**Valor unitário (R$)**	**Quantidade / Volume**	**Valor total (R$)**
1.	<Descrição igual do Termo de Referência>				
...					
				Total	

Cronograma:

O cronograma deve seguir o que está disposto no item "**4.3. Requisitos de Implantação"** do Termo de Referência que deu origem ao Contrato e deve acrescentar a coluna de datas limites preenchidas no momento da abertura da Ordem de Fornecimento de Bens e Serviços;

< Incluir aqui a tabela do item 4.3.1 do Termo de Referência, acrescentando a coluna "Datas Limites" >

Caso se refira a solicitação de treinamento, o cronograma deve seguir o que está disposto no item "**4.6.9.14. Cronograma de treinamento"** do Termo de Referência que deu origem ao Contrato e deve acrescentar a coluna de datas limites preenchidas no momento da abertura da Ordem de Fornecimento de Bens e Serviços;

< Incluir aqui a tabela do item 4.6.9.14 do Termo de Referência, acrescentando a coluna "Datas Limites" >

CIÊNCIA	
Área requisitante	**Gestor do contrato**
_____ <Requisitante> Matr.: <nº da matrícula> Local, <dia> de <mês> de <ano>	_____ <Gestor> CPF: <nº do CPF do preposto> Local, <dia> de <mês> de <ano>
CONTRATADA	
_____ <Preposto> CPF: <nº do CPF do preposto> Local, <dia> de <mês> de <ano>	

ANEXO I - E - TABELA DE CUMPRIMENTO DE REQUISITOS

Item	Descrição do item	Documento que comprova	Página
4.6.	**DOS REQUISITOS TÉCNICOS E FUNCIONAIS**	**-**	**-**
4.6.1.	**Considerações Gerais**	**-**	**-**
4.6.1.1.	O não atendimento a qualquer um desses requisitos é fator impeditivo para a habilitação da licitante.		
4.6.1.2.	A solução deverá oferecer condições para gestão dos dados não estruturados de diretório de usuários, servidores de arquivos e serviço		

	de e-mail, de forma que a equipe de TI da agência tenha condições de analisar, controlar e auditar os recursos e plataformas monitoradas.		
4.6.1.3.	A solução deverá fazer o monitoramento e auditoria dos usuários e seus acessos internos e externos ao diretório de usuários, pastas, arquivos e caixas de e-mail dos servidores monitorados.		
4.6.1.4.	O monitoramento e auditoria deverão gerar indicadores de performance para a gestão inteligente dos dados não estruturados, de forma que a agência possa evoluir e melhorar a performance, capacidade e segurança das informações e dos recursos monitorados.		
4.6.1.5.	Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo deverá ser executado de forma a diminuir o impacto sobre a disponibilidade dos serviços.		
4.6.1.6.	Devido à complexidade e à quantidade de servidores monitorados, todas as informações e plataformas monitoradas deverão ser apresentadas em uma única console integrada que atenda aos requisitos deste termo de referência e que deve ter seu acesso controlado por meio de autenticação baseada em usuários do domínio da agência.		
4.6.1.7.	Deve ser possível a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o acesso de analistas, equipe de suporte e usuários finais.		
4.6.1.8.	A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica.		
4.6.1.9.	Caso a solução seja compatível com sistemas operacionais Windows Server 2012 R2 ou superior ou distribuições linux gratuitas, não haverá necessidade do fornecimento de licenças.		
4.6.1.10.	A agência possui conhecimento e infraestrutura consolidada de banco de dados Microsoft SQL Server e Oracle. Portanto, a solução ofertada deverá reter as informações de log de acessos aos recursos monitorados em banco de dados Microsoft SQL Server ou Oracle. Nesse caso, não será necessário o fornecimento de licenças para o banco de dados.		
I.	Caso a solução fornecida seja incompatível com Microsoft SQL Server e Oracle, a contratada poderá utilizar outro sistema de banco de dados, desde que forneça todo o licenciamento do banco de dados necessário para a utilização da solução pela contratante. O licenciamento do banco de dados deve permitir seu uso pela solução de forma perpétua.		
4.6.1.11.	A solução deve permitir o acesso a, no mínimo, 10 anos de dados de auditoria capturados e armazenados.		
4.6.1.12.	A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização Microsoft Hyper-V.		
4.6.1.13.	Como a quantidade de servidores de arquivos, servidores de Exchange e controladores de domínio é variável, a solução deve ter escalabilidade para atender a quantidade crescente de servidores monitorados, sem a necessidade de aquisição de novas licenças.		
4.6.1.14.	Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia, a solução deverá ter		

	certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação, como a ISO/IEC 27.001 ou similares.		
4.6.1.15.	As soluções fornecidas pela contratada devem contemplar a auditoria de sistemas na última versão disponibilizada pelo fabricante.		
4.6.1.16.	As soluções fornecidas devem permitir auditar, controlar, monitorar e gerenciar as contas de 2.400 colaboradores da Agência.		
4.6.1.17.	As soluções fornecidas devem permitir auditar, controlar, monitorar e gerenciar 3.200 contas ativas do domínio.		
4.6.1.18.	A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos, exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.		
4.6.1.19.	Deve ser possível, através da console, a criação de modelos de relatórios para posterior reutilização. Essa criação de modelos deve ser intuitiva e não deve necessitar da utilização de linguagem de programação ou outro software.		
4.6.1.20.	A documentação relativa às especificações técnicas da solução de TI deve ser fornecida em Português. Alternativamente, poderá ser apresentada em Língua Inglesa.		
4.6.1.21.	O licenciamento fornecido para todos os sistemas ou ferramentas que compõe essa solução deve ser perpétuo, não podendo, portanto, ter prazo de expiração de uso ou limitação de funcionalidades em função do tempo.		
4.6.1.22.	A solução deve permitir o acesso de, pelo menos, 10 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que são disponibilizadas a todos os usuários da agência, a solução deve permitir o acesso de todos os usuários.		
4.6.1.23.	A solução deve possuir interface nos idiomas Português ou Inglês.		
4.6.1.24.	Todos os itens apresentados nesta especificação são obrigatórios e deverão ser atendidos de forma nativa. Entende-se por itens atendidos de forma nativa, todos aqueles itens atendidos diretamente pelo software e seus módulos, sem a necessidade de alteração do código fonte em sua estrutura.		
4.6.2.	**Características Gerais – Permissões**	**-**	**-**
4.6.2.1.	A solução deverá apresentar em sua interface todos os usuários e grupos de segurança dos diferentes domínios monitorados, assim como os usuários e grupos de segurança locais de cada servidor ou plataforma monitorada.		
4.6.2.2.	A solução deve permitir a busca por uma pasta nos servidores monitorados e apresentar quais usuários e grupos de segurança têm permissões e quais permissões esses objetos têm na pasta.		
4.6.2.3.	A solução deverá consolidar as permissões NTFS e Share de cada pasta e demonstrar a permissão efetiva dos usuários e grupos.		
4.6.2.4.	A solução deve utilizar os eventos coletados pela auditoria para realizar a análise comportamental automática dos usuários de maneira a fazer recomendações de revogação de acesso aos dados não estruturados dos		

	servidores monitorados.		
4.6.2.5.	Além da visibilidade de permissões, usuários e grupos de segurança, deve ser possível realizar alterações de permissionamento dos usuários e grupos de segurança às pastas e diretórios dos servidores monitorados através da interface gráfica da solução.		
4.6.2.6.	A solução deve fornecer a visibilidade sobre aplicação de alterações e o histórico das alterações aplicadas através da console. Deve oferecer ainda a possibilidade de restaurar determinada alteração realizada.		
4.6.3.	**Características Gerais - Logs de auditoria dos recursos monitorados**	**-**	**-**
4.6.3.1.	A solução deve coletar de forma automática e contínua logs de acessos a diretórios, pastas e arquivos dos servidores de arquivos monitorados, acessos a objetos do Active Directory (AD) e acessos a caixas postais do Exchange.		
4.6.3.2.	Deve ser possível, na interface gráfica da solução, visualizar os logs de auditoria de acessos a diretórios, pastas e arquivos dos servidores monitorados, acessos a objetos do AD e acessos a caixas postais do Exchange organizados e agrupados por recurso monitorado:		
I.	Pasta ou diretório: demonstrar todos os eventos para aquela pasta, subpastas e arquivos;		
II.	Unidade organizacional: demonstrar os eventos ocorridos em determinada OU;		
III.	Usuário ou grupo de segurança: demonstrar os eventos gerados ou sofridos por determinado usuário ou grupo.		
4.6.3.3.	Os eventos de auditoria coletados pela solução devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.		
4.6.3.4.	As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários, grupos de segurança e e-mails dos servidores monitorados.		
4.6.3.5.	Deve ser possível alterar também o conjunto de dados (colunas) retornados da consulta de auditoria de acordo com a necessidade da informação.		
4.6.3.6.	Todos os eventos dos diferentes servidores monitorados devem ser apresentados na mesma console gráfica da solução onde são também apresentadas as informações de permissionamento desses mesmos servidores monitorados.		
4.6.3.7.	A solução deve fornecer resumo das atividades auditadas, incluindo:		
I.	Quantidade de eventos por dia;		
II.	Visualização dos usuários mais e menos ativos nos servidores monitorados;		

III.	Visualização dos diretórios mais e menos acessados nos servidores monitorados;		
IV.	Visualização dos diretórios e pastas acessadas por um usuário ou grupo de segurança;		
V.	Visualização dos usuários inativos em uma pasta ou diretório.		
4.6.4.	**ITEM 1 - Licença perpétua de solução de auditoria e outras funcionalidades para serviço de diretório (Microsoft *Active Directory*).**	**-**	**-**
4.6.4.1.	As funcionalidades descritas nas características gerais devem se aplicar à solução para os serviços de diretórios de usuários do Microsoft Active Directory, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados.		
4.6.4.2.	A solução descrita neste item deve possuir as seguintes funcionalidades globais:		
I.	Auditar ações sobre objetos do Active Directory;		
II.	Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;		
III.	Gerar alerta com base nas informações auditadas;		
IV.	Automatizar tarefas repetitivas, comum ou complexas;		
V.	Monitorar e analisar comportamentos suspeitos de usuários.		
4.6.4.3.	A solução deve oferecer a visibilidade gráfica da estrutura hierárquica de todos os domínios, OUs e objetos monitorados no AD da agência, apresentados na mesma console em que apresenta seus logs de auditoria.		
4.6.4.4.	A solução deve suportar a demonstração gráfica e a auditoria de diferentes domínios.		
4.6.4.5.	Deverá suportar as tecnologias DAS, SAN e suporte à tecnologia de cluster da Microsoft.		
	Funcionalidade: auditar ações sobre objetos do *Active Directory*.	**-**	**-**
4.6.4.6.	A solução deverá fornecer informações detalhadas de auditoria para perícia em relação aos seguintes pontos:		
I.	Quem pode acessar e qual acesso pode fazer aos objetos do AD;		
II.	Quem faz alteração nos objetos;		
III.	Quem tem usado as credenciais para acessar os serviços de diretório;		
IV.	Detalhes dos eventos sobre objetos;		
V.	Quem possui permissões excessivas sobre os objetos;		
VI.	Quem deu ou revogou permissões de acesso e modificação.		

4.6.4.7.	A solução deverá ser capaz de rastrear quem fez alterações nos usuários, grupos, OUs e GPOs dos domínios monitorados do Active Directory, qual foi a alteração feita, quando foi feita, a máquina de origem da alteração e detalhes das propriedades tanto do objeto afetado quanto do objeto que gerou o evento.		
4.6.4.8.	A solução deverá indicar graficamente ou por relatório usuários ativos e inativos, usuários habilitados e desabilitados no AD.		
4.6.4.9.	A solução deve suportar a auditoria dos eventos do serviço de diretório, tais como:		
I.	Criação e deleção de todos os objetos;		
II.	Alteração de membros de grupos;		
III.	Alteração nas propriedades dos objetos do serviço de diretório;		
IV.	Requisições de acesso;		
V.	Autenticação de conta;		
VI.	Reconfiguração de senhas;		
VII.	Bloqueio e desbloqueio de conta;		
VIII.	Criação e deleção de conta;		
IX.	Habilitação e desativação de conta;		
X.	Eventos de permissão adicionada ou removida de objeto;		
XI.	Proprietário alterado;		
4.6.4.10.	A solução deve prover completa visibilidade sobre alterações em Objetos de Políticas de Grupos (GPO):		
I.	Modificação de configuração de GPOs;		
II.	Criação de link de GPO;		
III.	Deleção de link de GPO;		
IV.	Modificação de link de GPO.		
	Funcionalidade: gerar alerta com base nas informações auditadas e executar ações proativas, inclusive para múltiplos objetos do *Active Directory*.	**-**	**-**
4.6.4.11.	A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado syslog, eventlog, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.		
4.6.4.12.	A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:		

I.	Atividades anômalas;		
II.	Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos;		
III.	Escalações de privilégios não autorizadas;		
IV.	Detecção de ferramentas de intrusão ou malwares.		
4.6.4.13.	O sistema de alerta em tempo real deve ser capaz de alarmar atividades em Active Directory (elevação de privilégios, inclusão/exclusão de grupos e usuários).		
4.6.4.14.	A solução deve permitir a integração com sistemas de e-mail padrão de mercado, inclusive Microsoft Exchange 2013, para envio de e-mails (alertas, notificações) de forma automática, ou manual.		
	Funcionalidade: monitorar e analisar os comportamentos suspeitos de usuários.	-	-
4.6.4.15.	Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.		
4.6.4.16.	A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.		
4.6.4.17.	Através da análise comportamental, solução deve realizar a descoberta automática de contas privilegiadas como usuários administrativos e contas de serviço.		
4.6.4.18.	Deve ser contemplada a assinatura de uma base de conhecimentos do fornecedor atualizada mensalmente de alertas pré-configurados de eventos suspeitos tais como:		
I.	Ataques de sequestro de dados (ransomware);		
II.	Detecção de ferramentas nocivas ao ambiente;		
III.	Excessos de ações com acessos negados;		
IV.	Acessos indevidos dos administradores nos dados da empresa;		
V.	Excessivas tentativas de elevação de privilégios;		
VI.	Excesso de tentativas de autenticação ou contas bloqueadas;		
VII.	Excesso de atividades em dados parados e/ou inativos;		
VIII.	Alterações excessivas e anormais em GPO;		
IX.	Excesso de acessos em caixas postais de uma única máquina;		
X.	Excesso de ações em um curto espaço de tempo.		

4.6.4.19.	A solução deve entregar painel web que permita análise dos comportamentos e eventos suspeitos listados.		
4.6.4.20.	Deve possuir um painel web interativo identificando ações tais como:		
I.	Quantidade de alertas e suas severidades em determinado período;		
II.	Usuários se comportando de forma suspeita;		
III.	Tipos de alertas mais disparados;		
IV.	Máquinas mais utilizadas para as ações suspeitas;		
V.	Servidores, pastas e mailboxes que mais sofrem ações suspeitas;		
4.6.4.21.	O painel deve mostrar as propriedades do usuário do AD essenciais para a perícia do alerta gerado.		
4.6.4.22.	Para análise do usuário mais alertado, o painel deve possuir página que agregue todos os alertas gerados por aquele usuário, permitindo que seja identificado o cenário do possível ataque.		
4.6.4.23.	No painel, a partir de um alerta selecionado, a solução deve exibir página que liste todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser personalizável podendo ser filtrada, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.		
4.6.4.24.	A página com lista dos eventos deve apresentar gráfico que demonstre o quantitativo dos eventos em determinado período, para que seja possível identificar o desvio do comportamento indicado pela solução.		
4.6.4.25.	O painel deve fazer uma análise prévia dos alertas e correlacioná-los com outras informações e eventos do usuário alertado, dispositivo usado no momento do alerta, horário do evento.		
4.6.4.26.	Deve ser possível, a partir de selecionado evento alertado, fazer filtragem e correlacionamento com outros eventos como, por exemplo, o comportamento dos usuários do mesmo departamento do usuário alertado ou acessos ao mesmo tipo de informação sensível identificado pela solução.		
4.6.4.27.	O painel deve possuir página com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Exchange) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tais como:		
I.	Quantidade de usuários habilitados inativos, usuários desabilitados, usuários habilitados com senhas expiradas, usuários habilitados bloqueados, grupos vazios, grupos não-administrativos com usuários administradores;		
II.	Número total de grupos de segurança, contas de usuários e computadores;		
III.	Quantidade de usuários com recomendação de revogação de permissão excessiva feita pela auditoria;		
	Funcionalidade: relatórios	**-**	**-**

4.6.4.28.	A solução deve fornecer os seguintes relatórios:		
I.	Indicativos de uso de dados para a gestão de usuários, grupos de segurança e objetos do AD.		
II.	Logs de acessos e modificações de objetos do AD, com detalhamento dos eventos e metadados dos objetos afetados.		
III.	Todas as modificações de permissionamento de objetos dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de domínio.		
IV.	Alterações em grupos de segurança dos domínios monitorados.		
V.	Usuários inativos no domínio.		
VI.	Grupos de segurança vazios ou não utilizados.		
VII.	Usuários desabilitados que ainda fazem parte de grupos de segurança.		
VIII.	Histórico de membros de grupos de segurança.		
IX.	Estatísticas de autenticação e falha de autenticação.		
X.	Lista de usuários administradores em grupos não administrativos.		
XI.	Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental.		
XII.	Informações sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs dos domínios monitorados.		
4.6.5.	**ITEM 2 - Licença perpétua de sofwtare de solução de auditoria e outras funcionalidades para servidores de arquivos.**	**-**	**-**
4.6.5.1.	As funcionalidades descritas nas características gerais devem se aplicar para as soluções anteriores, e também para a solução de servidores de arquivos Windows.		
4.6.5.2.	A solução descrita neste item deve possuir as seguintes funcionalidades globais:		
I.	Auditar acesso, modificação e remoção de pastas e arquivos em servidores de arquivos;		
II.	Executar ações proativas com base na auditoria, inclusive para múltiplos objetos;		
III.	Gerar alerta com base nas informações auditadas;		
IV.	Automatizar tarefas repetitivas, comum ou complexas;		
V.	Permitir a delegação de gerenciamento de acessos aos proprietários dos dados;		
VI.	Monitorar e analisar comportamentos suspeitos de usuários.		

4.6.5.3.	A solução deve suportar como servidores de arquivos as versões do Windows Server 2008 ou versões superiores e Windows 7 e versões superiores.		
4.6.5.4.	A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios monitorados além de prever a possibilidade de criação de pastas e permissões para que a gestão do repositório seja centralizada.		
4.6.5.5.	A solução deve fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões.		
4.6.5.6.	A solução deve possuir compatibilidade comprovada no site do fabricante com storages EMC e HUAWEY, devendo possuir total compatibilidade com o ambiente da ANAC.		
4.6.5.7.	A interface gráfica da solução deverá permitir a busca por um usuário ou grupo de segurança e deverá apresentar suas permissões nas caixas postais e pastas dos servidores monitorados de forma integrada. As informações apresentadas incluem:		
I.	Identificação de herança de permissão ativada/desativada;		
II.	Indicação de existência de compartilhamento;		
III.	A fonte da permissão, ou seja, de que grupo o usuário está herdando a permissão.		
	Funcionalidade: permitir a delegação de gerenciamento de acesso aos proprietários dos dados	-	-
4.6.5.8.	A solução contratada deve oferecer um portal web integrado com os módulos de auditoria para que os proprietários das pastas tenham uma informação íntegra dos eventos de sua pasta.		
4.6.5.9.	A solução deverá permitir que os usuários donos das pastas concedam acesso às suas pastas ou grupos para outros usuários, bem como a revogação destes acessos, sem necessidade de envolvimento do administrador do sistema.		
4.6.5.10.	Deve fornecer método para assinalar ou associar um ou mais usuários como proprietário de uma pasta.		
4.6.5.11.	Uma vez realizada a requisição de nova credencial à pasta ou inclusão à um grupo, a solução ofertada deverá realizar as configurações no ambiente sem que haja o envolvimento do administrador do sistema.		
4.6.5.12.	Deve ter interface web para solicitação de permissionamento ou participação em grupo de segurança e acesso à pasta.		
4.6.5.13.	Deve ser capaz de personalizar um fluxo de aprovação para cada demanda do usuário, permitindo dois ou mais aprovadores simultâneos ou em série.		
4.6.5.14.	A solução deverá ser capaz de enviar e-mail de notificação ao aprovador/dono da informação quando uma nova solicitação for aberta a ele.		
4.6.5.15.	O portal deve possibilitar a escolha de uma data de expiração ou validade do permissionamento aprovado, e realizar a revogação automática da permissão quando chegar a data de expiração sem que se faça necessária a intervenção de um usuário.		

MINUTA

ANEXO II

TERMO DE CONTRATO

AQUISIÇÃO DE LICENÇAS E PRESTAÇÃO DE SERVIÇO DE INSTALAÇÃO, TREINAMENTO, GARANTIA E SUPORTE TÉCNICO

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº ...../...., QUE FAZEM ENTRE SI A AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL E A EMPRESA .....

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 ....., inscrito(a) no CPF nº ....., portador(a) da Carteira de Identidade nº ....., doravante denominada CONTRATANTE, e o(a) ..... inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ....., portador(a) da Carteira de Identidade nº ....., expedida pela (o) ....., e CPF nº ....., tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 2.271, de 7 de julho de 1997, e da Instrução Normativa SEGES/MPDG nº 5, de 26 de maio de 2017, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº ...../20...., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (*Microsoft Active Directory*), correio eletrônico (*Microsoft Exchange Server*) e servidores de arquivos (*Microsoft File Server*). A solução deve monitorar os usuários em tempo real, identificar desvios de comportamento, permitir delegação de gerenciamento de acesso aos proprietários dos dados, executar ações proativas em múltiplos objetos, e identificar e classificar conteúdos sensíveis. A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, conforme condições, quantidades e exigências estabelecidas neste instrumento, que serão prestados nas condições estabelecidas no Termo de Referência, anexo do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3. Objeto da contratação:

GRUPO	Item	Descrição da solução	Fabricante, especificação dos produtos e versão	Unidade	Quantidade	Valor Unitário (R$)	Valor total - ANO 1 (R$)	Valor Total - Demais anos (R$)	Valor Total* (R$) (3 anos)
1	1	Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft *Active Directory).*		Usuários	2.400				
	2	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de servidores de arquivos.		Usuários	2.400				
	3	Licença perpétua de software de solução de tecnologia da informação para auditoria e outras funcionalidades de correio eletrônico (*Microsoft Exchange)*.		Usuários	2.400				

GRUPO	Item	Descrição da solução	Fabricante, especificação dos produtos e versão	Unidade	Quantidade	Valor Unitário (R$)	Valor total - ANO 1 (R$)	Valor Total - Demais anos (R$)	Valor Total* (R$) (3 anos)
	4	Licença perpétua de software de solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis.		Usuários	2.400				
	5	Serviços de suporte técnico e garantia		meses	36				
	6	Treinamento para as soluções contratadas		turma	1				
Valor Total (R$)									

2. CLÁUSULA SEGUNDA – VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

2.1.1. Os serviços tenham sido prestados regularmente;

2.1.2. Esteja formalmente demonstrado que a forma de prestação dos serviços tem natureza continuada;

2.1.3. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.1.4. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.1.5. Seja comprovado que o valor do contrato permanece economicamente vantajoso para a Administração;

2.1.6. Haja manifestação expressa da contratada informando o interesse na prorrogação; e

2.1.7. Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.1.8. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

2.2. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

3. 3. CLÁUSULA TERCEIRA – PREÇO

3.1. O valor total da contratação é de R$..... (.....), sendo que apenas o item 5 terá pagamentos mensais no valor de R$..... (.....).

3.2. 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.

4. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 20...., na classificação abaixo:

Gestão/Unidade:

Fonte:

Programa de Trabalho:

Elemento de Despesa:

4.2. No(s) exercício(s) seguinte(s), correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

5. CLÁUSULA QUINTA – PAGAMENTO

5.1. O prazo para pagamento à CONTRATADA e demais condições a ele referentes encontram-se definidos no Edital e no Anexo XI da IN SEGES/MP nº 5/2017

6. CLÁUSULA SEXTA – REAJUSTE

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

6.1.1. Dentro do prazo de vigência do contrato, mediante solicitação da contratada e após o interregno de um ano, exclusivamente para o **item 5** relativo aos **serviços de suporte técnico e garantia,** os preços contratados poderão sofrer reajuste, aplicando-se o índice descrito no item 14.5 exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.2. O interregno mínimo de 1 (um) ano para o 1º (primeiro) reajuste de que trata o item antecedente será contado a partir da data limite para apresentação de propostas constante do instrumento convocatório, ou do orçamento a que a proposta se referir, em relação aos custos dos serviços de suporte técnico e garantia dispostos e/ou previstos na pertinente Proposta Comercial da Contratada.

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

6.4. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

6.5. O reajuste de que trata esta cláusula será efetuado com base no Índice de Custos de Tecnologia da Informação – ICTI, calculado e divulgado pelo Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, ou outro índice que venha a substituí-lo por força de determinação legal ou por sua falta ou descontinuidade.

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

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

6.8. 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.

6.9. O reajuste será realizado por apostilamento.

6.10. Quando da solicitação do reajuste de que trata esta Cláusula, este somente será concedido mediante a comprovação pela Contratada do aumento dos custos ali especificados, considerando-se:

6.10.1. a apresentação de nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo que retrata a variação dos custos específicos;

6.10.2. o adequado índice de que trata esta Cláusula, o qual retrate a variação dos preços relativos aos custos objeto do pretenso reajuste, desde que devidamente individualizados na mencionada Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo da Contratada;

6.10.3. a disponibilidade financeira e orçamentária do órgão ou entidade Contratante.

6.11. É vedada a inclusão na nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo previstos no item antecedente, por ocasião da solicitação do reajuste de que trata esta Cláusula, de materiais, equipamentos, componentes, peças, acessórios, produtos não previstos na originária Proposta Comercial da Contratada, exceto quando se tratar das situações e casos devidamente comprovados e acompanhados da respectiva justificativa e documentação comprobatória atestada pela procedente Equipe Técnica responsável pela pertinente Gestão e Fiscalização Contratual.

6.12. Não sendo juntada à solicitação de reajuste de que trata esta Cláusula a mencionada nova Planilha ou Memória de Cálculo ou Demonstrativo de Cálculo que retrata a variação dos custos específicos, o adequado índice de que trata esta mesma Cláusula, juntamente com a pertinente documentação comprobatória, a análise pela parte da Contratante ficará suspensa até a apresentação da devida documentação.

7. CLÁUSULA SÉTIMA – GARANTIA DE EXECUÇÃO

7.1. A CONTRATADA prestará garantia no valor de R$ ..... (.....), na modalidade de ....., , no prazo de 10 (dez) dias, observadas as condições previstas no Edital, com validade de 90 (noventa) dias após o término da vigência contratual, devendo ser renovada a cada prorrogação, observados os requisitos previstos no item 3.1 do Anexo VII-F da IN SEGES/MPDG n. 5/2017

Ou

7.1. A CONTRATADA, na assinatura deste Termo de Contrato, prestou garantia no valor de R$ ..... (.....), na modalidade de ....., , observadas as condições previstas no Edital, com validade de 90 (noventa) dias após o término da vigência contratual, devendo ser renovada a cada prorrogação , observados os requisitos previstos no item 3.1 do Anexo VII-F da IN SEGES/MPDG n. 5/2017.

8. CLÁUSULA OITAVA – REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. O regime de execução dos serviços a serem executados pela CONTRATADA, os materiais que serão empregados e a fiscalização pela CONTRATANTE são aqueles previstos no Termo de Referência, anexo do Edital.

9. CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

9.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas nos itens 5 e 6, respectivamente, do Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA – SANÇÕES ADMINISTRATIVAS.

10.1. As sanções relacionadas à execução do contrato são aquelas previstas no item 8.3 do Termo de Referência, anexo do Edital.

11. CLÁUSULA DÉCIMA PRIMEIRA – RESCISÃO

11.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo do Edital.

11.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

11.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

11.4. O termo de rescisão, sempre que possível, será precedido:

11.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

11.4.2. Relação dos pagamentos já efetuados e ainda devidos;

11.4.3. Indenizações e multas.

12. CLÁUSULA DÉCIMA SEGUNDA – VEDAÇÕES

12.1. É vedado à CONTRATADA:

12.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

12.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do ANEXO X da IN nº 05, de 2017.

13.2. A CONTRATADA é obrigada 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.

13.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14. CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

14.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 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.

15. CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei nº 8.666, de 1993.

16. CLÁUSULA DÉCIMA SEXTA – FORO

16.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Seção Judiciária de ..... - Justiça Federal.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

....., ... de..... de 20.....

_____

Representante legal da CONTRATANTE

_____

Representante legal da CONTRATADA

TESTEMUNHAS:

Nota Explicativa*: Necessário que tenha a assinatura do responsável legal da CONTRATANTE e da CONTRATADA e de 2 testemunhas para atender o disposto no art. 784, III do CPC que considera título executivo extrajudicial o documento particular assinado por duas testemunhas.*

1-

2-

Documento assinado eletronicamente por **Aderson de Lima Calazans**, **Analista Administrativo**, em 28/11/2019, às 09:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sistemas.anac.gov.br/sei/autenticidade, informando o código verificador **3774990** e o código CRC **4D2F87BD**.

AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL
SCS, Quadra 09, Lote C, Torre A - 1º Andar, Edifício Parque Cidade Corporate - Bairro Setor Comercial Sul, Brasília/DF, CEP 70308-200
Telefone: +55 (61) 3314-4154 - www.anac.gov.br

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. INTRODUÇÃO

A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de solução para gestão, monitoração, auditoria, automação e prevenção de perdas de dados nos serviços de diretório do *Active Directory* (AD), correio eletrônico (*Exchange*) e servidores de arquivos, bem como fornecer informações necessárias para subsidiar o respectivo processo.

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Solução de tecnologia da informação para auditoria e gerenciamento de serviços do AD (*Microsoft Active Directory*), correio eletrônico (*Microsoft Exchange Server*) e servidor de arquivos (*Microsoft File Server*), que realize monitoramento em tempo real e identifique desvios de comportamento dos usuários.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES

Esta sessão atende ao disposto na Instrução Normativa MP/SLTI nº 04/2014, art. 12, inciso I, que compreende a tarefa de definição e especificação das necessidades de negócio e tecnológicas, e/ou dos requisitos necessários e suficientes à escolha da Solução de Tecnologia da Informação.

3.1. NECESSIDADES DE NEGÓCIO

ID	Funcionalidades	Envolvidos
1.	Aumentar o nível de atendimento e qualidade das operações de serviços de TI.	STI
2.	Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos.	STI
3.	Automação de controle de privilégios aos curadores dos dados e informações.	STI
4.	Classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos.	STI
5.	Análise comportamental dos usuários internos no ambiente computacional reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados.	STI
6.	Aprimorar a governança de TI.	STI
7.	Aprimorar governança de dados, informação e conhecimento.	STI
8.	Aprimorar a gestão de segurança da informação e comunicações.	STI
9.	Disponibilização de segurança, auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos, e de sistemas de TI.	STI
10.	Pesquisas de auditoria referente a quem, quando, onde e como um dado é utilizado.	GEIT/STI
11.	Monitoramento eficiente de acessos aos dados armazenados	GEIT/STI
12.	Gerenciamento e auditoria eficientes do repositório de usuários e emails.	GEIT/STI
13.	Ações proativas em casos de incidentes de segurança cibernética e ataque de *malwares*.	GEIT/STI
14.	Identificação de acessos indevidos de usuários internos mal-intencionados.	GEIT/STI
15.	Aproveitamento eficiente do espaço de armazenamento dos eventos de auditoria	GEIT/STI
16.	Atendimento dos princípios e diretrizes estabelecidos na IN 115/2017, que institui a Política de Governança de Informações Digitais - PGID da ANAC.	STI
17.	Implementação de parte dos pontos destacados nas seções II, III e VII, do Capítulo IV, da IN 080/2014, que institui a Política de Segurança da Informação e Comunicações - PoSIC no âmbito da Agência Nacional de Aviação Civil - ANAC.	STI
18.	Alinhamento a padrões definidos no item 10.10 da ABNT NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação	STI
19.	Adequação a achados da Auditoria interna do processo de gestão de infraestrutura de TIC (Documento SEI nº 0898845), relacionado a deficiência nos procedimentos de segurança de redes e falha no processo de gestão de identidade.	STI

3.2. REQUISITOS TECNOLÓGICOS DA SOLUÇÃO

3.2.1. A solução para gestão, monitoração, auditoria, automação e prevenção de perdas de dados deve ser capaz de avaliar os seguintes serviços:

3.2.1.1. Base de armazenamento de informação sobre usuários, dispositivos e sistemas (*Active Directory*).

3.2.1.2. Correio eletrônico (*Microsoft Exchange*).

3.2.1.3. Servidores de arquivos (*Windows File Services*).

3.2.2. A solução deve possuir as seguintes funcionalidades:

3.2.2.1. Simplificar operações em lote de múltiplos objetos no AD, em servidores de arquivos ou no correio eletrônico.

3.2.2.2. Automatizar tarefas repetitivas, comuns ou complexas, associadas ao gerenciamento do AD.

3.2.2.3. Analisar o ambiente, coletar informações sobre objetos, arquivos e caixas de correio.

3.2.2.4. Gerar relatórios que permitam garantir a efetividade de controles de segurança, assim como uma visão do estado atual e histórico de usuários e acessos.

3.2.2.5. Permitir responder quem, quando, onde e como um determinado objeto foi acessado, editado ou excluído.

3.2.2.6. Permitir a identificação de tentativas ou acessos, aceitos ou rejeitados, de usuários, computadores ou sistemas.

3.2.2.7. Permitir identificar a frequência de utilização e o último acesso aos objetos e arquivos auditados.

3.2.2.8. Permitir identificar permissões de acesso ou de modificação não necessárias aos recursos, arquivos ou caixas de correio.

3.2.2.9. Permitir identificar a origem dos acessos a arquivos e objetos.

3.2.2.10. Permitir o acesso às informações de auditoria em tempo real ou em histórico de, no mínimo, 5 anos.

3.2.2.11. Permitir automatizar a identificação, a remoção de permissões, a desativação e a remoção de objetos e arquivos com base em informações de auditoria.

3.2.2.12. Detectar atividades não autorizadas de processamento de informações.

3.2.2.13. Permitir a configuração de alertas com base nas informações auditadas.

3.2.2.14. Permitir a auditoria de informações de acessos tanto de administradores quanto dos usuários dos serviços.

3.2.2.15. Utilizar de forma eficiente o espaço em disco necessário para armazenamento dos eventos de auditoria.

3.2.2.16. Utilizar as informações auditadas para sugerir melhorias no uso dos recursos.

3.2.2.17. Permitir a gestão eficiente dos recursos auditados.

3.2.2.18. Permitir a identificação e classificação de conteúdos sensíveis em servidores de arquivos.

3.2.2.19. Permitir a identificação dos proprietários dos dados, listas de distribuição e caixas de correio individuais ou corporativas.

3.2.2.20. Monitorar os eventos das caixas postais dos usuários e das pastas públicas.

3.2.2.21. A coleta de informações de auditoria não deve onerar o processamento nos servidores alvo.

3.2.2.22. Permitir o ajuste os diretórios com herança quebrada de permissões.

3.2.2.23. Assegurar que as autorizações são baseadas em necessidades de negócio.

3.2.2.24. Suportar a versão atual e posteriores do *Active Directory* (versão atual na ANAC: 2012 R2), do correio eletrônico (versão atual na ANAC: Exchange 2013) e do serviços de arquivos (versões atuais dos sistemas operacionais: Windows Server 2008 ou superior)

3.2.2.25. Permitir auditar aproximadamente 2.400 usuários da agência.

3.2.2.26. Permitir auditar aproximadamente 11.600 contas de usuários/sistemas, sendo 4.400 contas de usuários/sistemas ativos no AD.

3.2.2.27. Permitir auditar aproximadamente 8.600 grupos do AD.

3.2.2.28. Permitir auditar aproximadamente 3.500 objetos de computadores do AD.

3.2.2.29. Permitir auditar aproximadamente 35.000 objetos diversos do AD.

3.2.2.30. Permitir auditar aproximadamente 20 servidores de arquivos existentes no ambiente da ANAC, que armazenam aproximadamente 26 TeraBytes de dados.

3.2.2.31. Permitir auditar 10 servidores do Exchange, que incluem 4 servidores de caixas de correio, 4 servidores de acesso e 2 servidores de borda.

3.2.2.32. Permitir auditar aproximadamente 3.800 caixas de correio eletrônico.

3.2.2.33. Suportar a utilização de servidores virtualizados para todos os seus componentes.

3.2.2.34. Monitorar diferentes domínios, independente da existência de relação de confiança.

3.2.2.35. Gerar relatórios de todas as consultas e ações feitas pelos usuários através da interface gráfica da solução, de modo que também seja possível realizar auditoria.

Os recursos solicitados para esta solução permitirão aumentar o nível de proteção das informações, ajudar na organização administrativa do AD, eliminar erros e agilizar o trabalho da TI na execução dessas atividades.

3.3. **DEMAIS REQUISITOS**

1	**Legais**	A demanda ora apresentada deve estar em conformidade com a legislação federal e normas internas (Decreto-Lei 200/67; Lei nº 8.666/93; Instrução Normativa SLTI/MP nº 04/2014; Plano Plurianual - PPA, Planejamento Estratégico Institucional – PEI ou Plano Diretor de Tecnologia da Informação – PDTI.)
2	**Segurança**	Atendimento à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Deve estar de acordo com as normas de Segurança da Informação da Agência, que estejam atualmente em vigor Permitir atender os padrões de referência estabelecidos nas normas ABNT NBR ISO/IEC 27002:2013. Atender
3	**Temporais**	A solução deverá ser entregue e instalada em até 90 (sessenta) dias, contados da data de assinatura do contrato.
4	**Manutenção**	A solução fornecida deverá possuir garantia e suporte técnico por de 36 meses. Este prazo é necessário para garantir que a solução continuará atualizada à medida que forem surgindo novas versões dos softwares auditados e, além

		disso, para garantir seu completo funcionamento durante um período de vida útil mínimo para o produto. Aliado a isso, verifica-se ainda que diversas outras contratações relacionadas a esse tipo de solução tem por padrão a contratação dos serviços de suporte e garantia pelo prazo solicitado.
5	**Capacitação**	Tendo em vista que a solução a ser adquirida contemplará soluções modernas, com novos recursos e funcionalidades, e ainda não utilizadas pela Agência, verifica-se a necessidade de atualização da equipe técnica da ANAC por meio de treinamento e capacitação.

4. LEVANTAMENTO DAS ALTERNATIVAS

Em atendimento ao disposto na Instrução Normativa MP/SLTI nº 04/2014, art. 12, inciso II, realiza-se agora a avaliação de soluções e a capacidade de cada uma das soluções para atender aos requisitos.

4.1. Desenvolvimento próprio de sistemas, scripts ou outro meio que permita obter as informações necessárias.

Cenário	
Entidade	Agência Nacional de Aviação Civil
Descrição	Desenvolvimento próprio na Agência através de contratos com empresas especializadas na prestação do serviço de desenvolvimento de sistemas e portais, ou criação pela equipe de suporte de scripts para o atendimento das necessidades.
Fornecedor	Contrato de suporte de 3 nível, caso a opção seja por scripts próprios. Utilização da fábrica de software contratada pela agência.
Análise da Solução	Dentro do ambiente da ANAC, vários scripts foram criados nos últimos 11 anos com a finalidade de capturar parte da informação de log existente nos ambientes do *Active Directory, Exchange* e servidores de arquivos e obter informações úteis do ponto de vista de auditoria. Mesmo com a utilização de diversos scripts e de várias ferramentas providas juntamente com o AD para gerenciar dados e políticas, percebe-se uma necessidade cada vez maior de funcionalidades para gerenciamento, auditoria e relatórios, e uma grande dificuldade em atender as necessidades com a utilização de scripts. Normalmente, esse tipo de trabalho é demorado, com custo alto e desvia o foco da TI no atendimento de demandas finalísticas da instituição. Com base nessas informações, a opção de desenvolvimento de scripts para o atendimento das necessidades torna-se inviável para a Agência. Em se tratando da possibilidade de desenvolvimento de uma nova solução com a utilização da fábrica de software contratada pela Agência, vale a pena destacar que o Ministério do Planejamento, Orçamento e Gestão, através da Secretaria de Tecnologia da Informação, orienta na publicação "*Boas práticas, vedações e orientações para contratação de serviços de desenvolvimento e manutenção de software (Fábrica de Software)*", disponível em desenvolvimento e manutenção de software, o seguinte: 1. Antes de decidir ... pela abertura de projetos de desenvolvimento de software, a Equipe de Planejamento da Contratação ou a Equipe de Gestão de Projetos do órgão deve realizar Estudo Técnico Preliminar, nos termos do disposto no art. 12 da Instrução Normativa SLTI/MP nº 4, de 11 de setembro de 2014, e executar as seguintes atividades: ... 1.5. Analisar a viabilidade de contratação de software proprietário. ... 2.5. É vedada a utilização dos serviços contratados para o desenvolvimento de softwares de atividades meio. 2.5.1. São considerados softwares de atividades meio os que são utilizados para apoio de atividades de gestão ou administração operacional, como, por exemplo, softwares de recursos humanos, ponto eletrônico, portaria, biblioteca, gestão de patrimônio, controle de frotas, gestão eletrônica de documentos, e não têm por objetivo o atendimento às áreas finalísticas para a consecução de políticas públicas ou programas temáticos. 2.5.2. Os softwares de atividades meio devem ser adquiridos no mercado por meio de adoção de software público ou livre, contratação de software como serviço, ou software licenciado. O desenvolvimento de uma solução para atender ao objetivo desse estudo está alinhada à vedação exposta no item 2.5 da orientação citada acima. Diante do exposto, não é recomendado o desenvolvimento interno de uma solução deste porte. Além disso, vale destacar que o custo-benefício para desenvolvimento interno de uma solução deste porte e com todas as funcionalidades necessárias não seria é viável tecnicamente e economicamente.

4.2. Disponibilidade de solução similar em outro órgão ou entidade da Administração Pública.

Considerando a dificuldade em obter as funcionalidades desejadas a partir do desenvolvimento interno da solução, muitos órgãos tem optado pela contratação diretamente no mercado.

Foram identificadas as seguintes contratações no ambiente de governo para o tipo de solução avaliado:

- **Agência Nacional de Transportes Terrestres - ANTT (Pregão Eletrônico nº 38/2018)**
  - **Objeto:** registro de preços para fornecimento e implantação de solução de auditoria e gerenciamento de serviços (*Microsoft Active Directory – AD*), servidor de arquivos (*Microsoft File Server*), correio eletrônico (*Microsoft Exchange Server*) e solução de análise de comportamento e alarme em tempo real, de uso permanente, incluindo a execução de serviços especializados de apoio pós-implantação, conforme condições, quantidades e especificações contidas no Termo de Referência, Anexo I do Edital.
  - **Itens do pregão:**
    - Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de AD (*Microsoft Active Directory*)
      - **Produto ofertado:** DatAdvantage for Microsoft Active Directory
      - **Custo:** R$ 2.264.400,00, ou R$ 444,00 por usuário, para 5.100 usuários

        - Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de servidores de Arquivos (Microsoft File Server)
            - **Produto ofertado:** DatAdvantage for Microsoft File Server
            - **Custo:** R$ 2.626.500,00, ou R$ 515,00 por usuário, para 5.100 usuários
        - Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de sistema de correio eletrônico (Microsoft Exchange Server)
            - **Produto ofertado:** DatAdvantage for Microsoft Exchange Server
            - **Custo:** R$ 2.907.000,00, ou R$ 570,00 por usuário, para 5.100 usuários
        - Solução de Tecnologia da Informação de análise de comportamento e alarme em tempo real
            - **Produto ofertado:** DatAlert
            - **Custo:** R$ 2.907.000,00, ou R$ 570 por usuário, para 5.100 usuários.
        - 1900 horas de serviços especializados de apoio pós-implantação
            - **Custo:** R$ 456.000,00, ou R$ 240,00 por hora.
        - **Adjudicado para:** OMEGA TECNOLOGIA DA INFORMACAO LTDA
- **Análise:** esta contratação está alinhada à necessidade levantada pela ANAC, exceto quanto ao item 4 das necessidades de negócio descritas no tópico 3.1 deste estudo.

- **Ministério Público do Trabalho/Procuradoria Geral do Trabalho - MPT/PGT (Pregão MPT/PG/39/2017)**
    - **Objeto:** registro de preços para a contratação de empresa especializada no fornecimento de subscrições, com vigência de 12 meses, de software para a auditoria de serviço de diretório *Microsoft Active Directory*, Servidor de Arquivos *Windows Server* e portal de autoatendimento para gestão de senhas de usuários, para atender às necessidades do Ministério Público do Trabalho, conforme descrições e quantitativos especificados no Edital e seus anexos;
    - **Itens do pregão:**
        - Pacote de subscrição anual de software para auditoria de serviço de diretório Microsoft *Active Directory* que atenda, no mínimo, 160 controladores de domínio e 7 mil contas de usuário.
            - **Produto ofertado:** *Netwrix Auditor for Active Directory*
            - **Custo:** R$ 50.024,35
        - Pacote de subscrição anual de software para auditoria de servidor de arquivos *Windows Server* que atenda, no mínimo, 160 servidores de arquivos Windows Server e 7 mil contas de usuário.
            - **Produto ofertado:** *Netwrix Auditor for File Services*
            - **Custo:** R$ 30.019,25
        - Treinamento para as soluções dos itens 1 e 2.
            - **Custo:** R$ 179,00 por participante
        - Prestação de serviços especializados para instalação e configuração das soluções ofertadas nos itens 1 e 2, com duração de 20 horas.
            - **Custo:** *R$* 4.896,35
        - **Adjudicado para:** AIQON SERVICOS EM INFORMATICA LTDA - ME
    - **Análise:** esta contratação não está alinhada à necessidade levantada pela ANAC, pois não atende as necessidades de negócio descritas nos itens 3, 4, 5 e 13 do tópico 3.1 deste estudo.

- **Ministério da Educação/Instituto Nacional de Estudos e Pesquisas Educacionais - MEC/INEP (Pregão 04/2017)**
    - **Objeto:** registro de preços para fornecimento e implantação de solução de auditoria e governança, baseado em software, para ambiente de diretórios de usuários, servidores de arquivos, correio eletrônico *Exchange*, monitoramento e prevenção de ameaças internas, identificação e classificação de informações sensíveis e automação de permissionamento no âmbito do Inep, contemplando execução de serviços de apoio pós-implantação.
    - **Itens do pregão:**
        - Solução de auditoria, controle e gerência de permissionamento dos serviços de AD (*Microsoft Active Directory*) para 1000 usuários com 36 meses de garantia.
            - **Produto ofertado:** Varonis - DatAdvantage for Directory Services & DatAdvantage Probe SL50
            - **Custo:** R$ 327,00 por usuário.
        - Solução de auditoria, controle e gerência de permissionamento dos serviços de servidores de Arquivos (*Microsoft File Server*) para 1000 usuários com 36 meses de garantia.
            - **Produto ofertado:** Varonis - DatAdvantage IDU Analytics (Engine) for Windows
            - **Custo:** R$ 667,00 por usuário.
        - Solução de auditoria, controle e gerência de permissionamento dos serviços de sistema de correio eletrônico (*Microsoft Exchange Server*) para 1000 caixas postais com 36 meses de garantia.
            - **Produto ofertado:** Varonis - DatAdvantage for Exchange

        - **Custo:** R$ 660,00 por usuário.
    - Solução de análise de comportamento e alarme em tempo real de ameaças internas para 1000 usuários com 36 meses de garantia.
        - **Produto ofertado:** Varonis - DatAlert Suite
        - **Custo:** R$ 665,00 por usuário.
    - Solução de classificação para 1000 usuários com 36 meses de garantia.
        - **Produto ofertado:** Varonis - IDU Classification Framework
        - **Custo:** R$ 663,00 por usuário.
    - Portal de permissionamento automático para 1000 usuários com 36 meses de garantia.
        - **Produto ofertado:** Varonis - *DataPrivilege*
        - **Custo:** R$ 668,00 por usuário.
    - 1.000 horas de serviços de apoio pós-implantação pelo período de 36 meses.
        - **Custo:** R$ 248,00 por hora.
    - **Adjudicado para:** OMEGA TECNOLOGIA DA INFORMACAO LTDA
- **Análise:** esta contratação está alinhada à necessidade levantada pela ANAC, pois atende às necessidades de negócio descritas no tópico 3.1 deste estudo.

- **Conselho Federal de Engenharia Arquitetura e Agronomia - CONFEA (Pregão 03/2017)**
    - **Objeto:** contratação de empresa especializada para fornecimento e instalação de Solução de Auditoria e Gerenciamento de Serviços do AD (*Microsoft Active Directory*), Servidor de Arquivos (*Microsoft File Server*), Correio Eletrônico (*Microsoft Exchange Server*), Solução de Portal de Permissionamento Automático, Solução de Classificação de Dados Sensíveis e Solução de Análise em tempo real e prevenção de comportamentos suspeitos, incluindo, treinamento para operacionalização do software, bem como execução de serviços de planejamento, implementação e testes, além de transferência de conhecimentos e operação assistida, com garantia (manutenção e suporte técnico), de acordo com as especificações e condições gerais constantes neste Edital e seus Anexos.
    - **Itens do pregão:**
        - Solução de Auditoria em *Microsoft Active Directory*
            - **Produto ofertado:** Varonis - DatAdvantage for Directory Services & DatAdvantage Probe SL50
            - **Custo:** R$ 200,00 por usuário.
            - **Quantidade:** 6.375 usuários
        - Solução de Auditoria em Microsoft Exchange
            - **Produto ofertado:** Varonis - DatAdvantage for Exchange
            - **Custo:** R$ 260,00 por usuário.
            - **Quantidade:** 6.375 usuários
        - Solução de Auditoria em Windows File Server
            - **Produto ofertado:** Varonis - DatAdvantage IDU Analytics (Engine) for Windows
            - **Custo:** R$ 287,90 por usuário.
            - **Quantidade:** 6.375 usuários
        - Solução de Portal de Permissionamento Automático
            - **Produto ofertado:** Varonis - *DataPrivilege*
            - **Custo:** R$ 290,00 por usuário.
            - **Quantidade:** 7.125 usuários
        - Solução de Classificação de Dados Sensíveis
            - **Produto ofertado:** Varonis - IDU Classification Framework
            - **Custo:** R$ 291,67 por usuário.
            - **Quantidade:** 7.125 usuários
        - Solução de análise em tempo real e prevenção de comportamentos suspeitos
            - **Produto ofertado:** Varonis - DatAlert Suite
            - **Custo:** R$ 293,33 por usuário.
            - **Quantidade:** 7.125 usuários
        - Serviços de garantia junto ao fabricante software com todas as características detalhadas para *Microsoft Active Directory*, pelo período de 12 (doze) meses.
            - **Custo:** R$ 50,00 por usuário.
            - **Quantidade:** 7.125 usuários
        - Serviços de garantia junto ao fabricante software com todas as características detalhadas para *Microsoft Exchange Server*, pelo período de 12 (doze) meses
            - **Custo:** R$ 65,00 por usuário.

        - **Quantidade:** 7.125 usuários
    - Serviços de garantia junto ao fabricante software com todas as características detalhadas para Microsoft Windows Server, pelo período de 12 (doze) meses
        - **Custo:** R$ 72,00 por usuário.
        - **Quantidade:** 7.125 usuários
    - Serviços de garantia junto ao fabricante software com todas as características para Portal de Permissionamento Automático, pelo Período de 12 meses
        - **Custo:** R$ 72,50 por usuário.
        - **Quantidade:** 7.125 usuários
    - Serviços de garantia junto ao fabricante software com todas as características para Solução de classificação de dados sensíveis, pelo Período de 12 meses
        - **Custo:** R$ 72,50 por usuário.
        - **Quantidade:** 7.125 usuários
    - Serviços de garantia junto ao fabricante software com todas as características para solução Análise em tempo real e prevenção de comportamentos suspeitos, pelo Período de 12 meses
        - **Custo:** R$ 72,50 por usuário.
        - **Quantidade:** 7.125 usuários
    - Operação Assistida (HORA)
        - **Custo:** R$ 249,50 por hora.
        - **Quantidade:** 3.300 horas
    - Treinamento Oficial do Fabricante para 3 (três) funcionários
        - **Custo:** R$ 6.000,00 por 3 participantes.
        - **Quantidade:** 15
    - **Adjudicado para:** INFOSEC TECNOLOGIA DA INFORMACAO LTDA
        - **Custo total: R$** 15.053.175,00
- **Análise:** esta contratação está alinhada à necessidade levantada pela ANAC, pois atende às necessidades de negócio descritas no tópico 3.1 deste estudo.

- **Ministério Público do Estado de Mato Grosso/Procuradoria Geral de Justiça - MP/PGT (Pregão 077/2016)**
    - **Objeto:** contratação de empresa especializada para fornecimento e instalação da Solução de Auditoria e Gerenciamento de Serviços do AD (*Microsoft Active Directory*), servidor de Arquivos (*Microsoft File Server*) e Correio Eletrônico (*Microsoft Exchange Server*), incluindo, transferência de conhecimentos e treinamento para operacionalização do software, bem como execução de serviços de planejamento, implementação e testes, com garantia de atualizações e suporte técnico pelo prazo de 12 meses e demais licenciamentos necessários ao funcionamento da Solução.
    - **Itens do pregão:**
        - Licenciamento da solução de auditoria para AD (*Microsoft Active Directory*) com Serviços de Garantia e suporte do Fabricante
            - **Produto ofertado:** NetAdmin automação e auditoria para *Active Directory* v4.3
            - **Custo:** R$ 264,96 por usuário.
            - **Quantidade:** 500 usuários
        - Licenciamento da solução de auditoria para Servidor de Arquivos (*Microsoft File Server*) com Serviços de Garantia e suporte do Fabricante
            - **Produto ofertado:** NetAdmin auditoria para *File Server v4.3*
            - **Custo:** R$ 336,00 por usuário.
            - **Quantidade:** 500 usuários
        - Licenciamento da solução de auditoria para Correio Eletrônico (*Microsoft Exchange Server*) com Serviços de Garantia e suporte do Fabricante
            - **Produto ofertado:** NetAdmin automação e auditoria para *Exchange Server* v4.3
            - **Custo:** R$ 336,00 por usuário.
            - **Quantidade:** 1.200 usuários
        - Banco de Horas de Consultoria para Implementações
            - **Custo:** R$ 2501,00 por hora.
            - **Quantidade:** 200 horas
        - **Adjudicado para:** Egon Tecnologia
        - **Custo total da contratação:** R$ 753.680,00
    - **Análise:** esta contratação não está alinhada à necessidade levantada pela ANAC, pois não atende as necessidades de negócio descritas nos itens 3, 4, 5 e 13 do tópico 3.1 deste estudo.

- **Governo do Estado de Rondônia/Departamento Estadual de Trânsito - DETRAN/RO (Pregão 027/2016/DETRAN/RO)**
  - **Objeto:** aquisição de licença de software de auditoria, controle e gerência de logs e permissionamento dos serviços de AD (*Microsoft Active Directory*), Servidor de Arquivos (*Microsoft File Server*) e Servidor de Atividades de Logon e Logoff, para ambiente Microsoft com instalação e treinamento *Hand's-ON*, garantia e suporte do fabricante por um período de 36 (trinta e seis) meses de garantia e suporte do fabricante por um período de 36 (trinta e seis) meses, de modo a atender às necessidades do DETRAN/RO, de acordo com a justificativa, quantidades e especificações técnicas mínimas constantes no TERMO DE REFERÊNCIA.
  - **Itens do pregão:**
    - Licença de software de auditoria e gerência de logs e permissionamento dos serviços de AD (*Microsoft Active Directory*)
      - **Produto ofertado:** Dell Change Auditor for Active Directory
      - **Custo:** R$ 190,00 por usuário.
      - **Quantidade:** 1.600 usuários
    - Servidor de arquivos (*Microsoft File Server*)
      - **Produto ofertado:** Dell Change Auditor for Windows File Servers
      - **Custo:** R$ 190,00 por usuário.
      - **Quantidade:** 1.600 usuários
    - Servidor de atividades de *logon* e *logoff*
      - **Produto ofertado:** Dell Change Auditor for logon activity
      - **Custo:** R$ 214,96 por usuário.
      - **Quantidade:** 1.600 usuários
    - **Adjudicado para:** RL2 Serviço de informática Ltda.
    - **Custo total da contratação:** R$ 594.960,00
  - **Análise:** esta contratação não está alinhada à necessidade levantada pela ANAC, pois não atende as necessidades de negócio descritas nos itens 3, 4, 5 e 13 do tópico 3.1 deste estudo. Além disso, a ferramenta Change Auditor, que antes era fornecida pela Dell, agora é fornecida pela empresa Quest. Por isso, essa contratação não serviria como base de comparação de custos com outras contratações.

- **Tribunal Superior Eleitoral - TSE (Pregão 125/2014)**
  - **Objeto:** aquisição de Solução de Auditoria em Ambiente Microsoft**,** com garantia de atualizações e suporte técnico pelo período de 36 (trinta e seis) meses, conforme especificações, condições, quantidades e prazos constantes do Termo de Referência - Anexo I deste edital.
  - **Itens do pregão:**
    - Fornecimento do software com todas as características detalhadas para *Microsoft Directory* (AD), pacote para 500 usuários internos.
      - **Produto ofertado:** Varonis
      - **Custo:** R$ 496.427,00 para 500 usuários.
      - **Quantidade:** 4 pacotes
    - Fornecimento do software com todas as características detalhadas para *Microsoft Windows Server*, pacote para 500 usuários internos.
      - **Produto ofertado:** Varonis
      - **Custo:** R$ 929.799,00 para 500 usuários.
      - **Quantidade:** 4 pacotes
    - Fornecimento do software com todas as características detalhadas para *Microsoft Exchange Server*, pacote para 500 caixas postais.
      - **Produto ofertado:** Varonis
      - **Custo:** R$ 1.372.680,96 para 500 usuários.
      - **Quantidade:** 4 pacotes
    - Serviços profissionais de implantação e testes para a solução.
      - **Custo:** R$ 124.567,00
      - **Quantidade:** 1
    - Serviços profissionais de transferência de conhecimento da solução, por participante.
      - **Custo:** R$ 38.805,00 por participante.
      - **Quantidade:** 7 participantes.
    - Serviços de suporte técnico para todos os softwares da solução e serviços executados, 8x5, pelo período de 36 (trinta e seis) meses, para a solução.
      - **Custo:** R$ 5.367,00 por mês
    - Serviços de garantia junto ao fabricante – software com todas as características detalhadas para *Microsoft Active Directory (*AD), pelo

período de 36 (trinta e seis) meses, pacote para 500 usuários internos.

- **Custo:** R$ 193.308,00para 500 usuários.
- **Quantidade:** 4 pacotes.

- Serviços de garantia junto ao fabricante – software com todas as características detalhadas para *Microsoft Windows Server*, pelo período de 36 (trinta e seis) meses, pacote para 500 usuários internos.
  - **Custo:** R$ 330.691,00 para 500 usuários.
  - **Quantidade:** 4 pacotes.
- Serviços de garantia junto ao fabricante – software com todas as características detalhadas para *Microsoft Exchange Server*, pelo período de 36 (trinta e seis) meses, pacote para 500 usuários internos.
  - **Custo:** R$ 489.003,00 para 500 usuários.
  - **Quantidade:** 4 pacotes.
- Serviços de Apoio pós-implantação pelo período de 36 (trinta e seis) meses, por hora para a solução. Incluem: Operação assistida, integração com novas versões do *Windows* e do *Exchange*, integração com sistemas do TSE e estudos de caso.
  - **Custo:** R$ 112.882,00.
  - **Quantidade:** 500.
- **Adjudicado para:** Vert Solucões em informática Ltda.
- **Custo total da contratação:** R$ 4.093.529,96

- **Análise:** esta contratação não está alinhada à necessidade levantada pela ANAC, pois não atende as necessidades de negócio descritas nos itens 3, 4, 5 e 13 do tópico 3.1 deste estudo.

Tomando por base as contratações apresentadas acima, é possível identificar as soluções das empresas Varonis, Dell, NetAdmin e Netwrix. Estas soluções e outras serão apresentadas mais à frente neste estudo.

4.3. Soluções existentes no portal do Software Público Brasileiro

Em consulta ao portal do software público brasileiro (https://softwarepublico.gov.br/social/), realizada em 30/07/2018, não foram identificadas soluções de auditoria para ambientes de Microsoft Exchange Server, servidores de arquivos e Microsoft Active Directory que atendessem aos requisitos técnicos e de negócio necessários.

4.4. Capacidade e alternativas do mercado

Atualmente existem duas alternativas de mercado para soluções de tecnologia da informação: disponibilidade de solução livre ou aquisição de software proprietário.

4.4.1. Soluções de software livre

Software livre é software que vem com permissão para qualquer um copiar, usar e distribuir, com ou sem modificações, gratuitamente ou por um preço. Em particular, isso significa que o código-fonte deve estar disponível. A maioria dos softwares livres é licenciada através de uma licença livre, sendo a GNU GPL a mais conhecida. As licenças de software livre permitem que eles sejam vendidos, mas estes em sua grande maioria estão disponíveis gratuitamente.

Abaixo são apresentadas as soluções de software livre relacionadas ao objeto deste estudo.

Nome da solução	Descrição e funcionalidades.
Pilha ELK www.elastic.co	A solução da pilha ELK, que é um acrônimo dos projetos de software livre *Elasticsearch*, *Logstash* e *Kibana, é* um conjunto de ferramentas extremamente poderoso e flexível que realiza a agregação de dados de diversas fontes, em vários formatos, e permite realizar buscas, análises e visualizações em tempo real. Trata-se de uma ferramenta de propósito geral, que poderia atender algumas das necessidades elencadas, mas que demandaria um trabalho grande de customização de relatórios e painéis para a obtenção das informações necessárias. Ainda assim, não seria capaz de atender a todas as necessidades de negócio e tecnológicas. Há diversos desafios na utilização desta ferramenta para a auditoria de AD, servidores de arquivos e correio eletrônico: • Vários relatórios não estão disponíveis na versão gratuita • A construção de painéis e consultas envolve um alto esforço e dedicação. • A difícil a manutenção de backups e histórico de informações na versão gratuita • Tem alto uso de armazenamento • Possui limitação na definição de perfis de acesso • Alto custo para customizações e adequação ao propósito • Necessidade de contratação de versão empresarial e suporte Apesar de ser um ferramenta muito útil, ela não conseguiria atender todas as necessidades e teria também alto custo associado a customização.
Graylog www.graylog.org	Trata-se de uma ferramenta gratuita corporativa de gerenciamento de todo tipo de registros de logs. Possui as seguintes funcionalidades: • Coleta e processamento de eventos de vários tipos de dados. • Armazena registro de ações tomadas pelo usuário • Permite monitoramento em tempo real de eventos.

Nome da solução	Descrição e funcionalidades.
	• Permite a criação de consultas personalizadas para analisar e pesquisar entre os dados coletados. • Permite investigar atividade de usuários suspeitos na última hora. • Permite a criação de painéis para visualizar métricas e observar tendência em uma interface única. • Permite adicionar novos gráficos e monitorar informações específicas. • Dispara ações ou notificações para eventos diversos por e-mail, ou ações por script para outros tipos de atividades. • Na versão gratuita, permite o armazenamento de até 5GB de dados por dia. • A versão *enterprise*, ou seja, com custo, permite arquivamento automático de dados de log e a recuperação caso seja necessário. • A versão *enterprise*, ou seja, com custo, permite auditoria de ações de usuários na base de dados. • A versão *enterprise*, ou seja, com custo, estende as funcionalidades da ferramenta. • Por fazer a coleta de logs, a ferramenta permitiria monitorar logs de eventos do Active Directory, dos servidores de arquivos e também do Exchange. Apesar de ser uma ferramenta com muitos recursos, também apresenta desafios similares ao descritos para o conjunto de ferramentas da pilha ELK e, assim, sua adoção pela ANAC, não conseguiria atender todas as necessidades e teria alto custo associado à customização de relatórios.
Active Directory Security Audit Tool Empresa: Paramount Defenses www.paramountdefenses.com	A Paramount Defenses é uma empresa que fornece diversas soluções de auditoria focadas no acesso ao Active Directory. Uma das soluções fornecida é a "Active Directory Security Audit Tool", que é uma ferramenta dentre o conjunto de oito soluções da "Gold Finger Active Directory Audit Tool Suite". A ferramenta gratuita da solução agrega as seguintes funcionalidades: • Auditoria de todas as contas de usuário do domínio, incluindo contas ativas, inativas, expiradas, travadas, administrativas ou contas filtradas por pesquisa LDAP customizada. • Auditoria de todas as contas de computadores do domínio, incluindo contas de controladores de domínio, ativas, inativas, sistemas operacionais e outras. • Auditoria de grupos de segurança, incluindo grupos nativos, de domínio local, globais, universais, vazios e administrativos. • Auditoria de unidades organizacionais (OU), pontos de conexão de serviço, filas de impressão, contatos e cotas. • Informação sobre os horários corretos do último *logon* e *logoff* de usuários e contas de computadores, além do controlador de domínio no qual a conta se conectou. As ferramentas pagas da soluções agregariam também diversas outras capacidades à solução, inclusive geração de diversos relatórios de auditoria pré-configurados. Trata-se de um conjunto de soluções que poderia atender vários requisitos associados a auditoria de Active *Directory*, no entanto, não atenderia requisitos associados a auditoria de servidores de arquivos e do ambiente de correio eletrônico. Por isso, não se trata de uma solução que atenda às necessidades da Agência.

Tabela 1 - Soluções livres.

Existem outros softwares livres ou softwares públicos que poderiam fornecer parte dos requisitos levantados pelo requisitante da solução, porém não há uma ferramenta de uso gratuito que atenda toda a necessidade ou grande parte dos requisitos de negócio e tecnológicos levantados pelo requisitante da solução.

4.4.2. **Soluções de software proprietário**

Nesta sessão serão levantadas e descritas soluções de software proprietário identificadas através de buscas na Internet ou pela leitura de estudos de mercado desenvolvidos pela empresa Gartner.

O Gartner é uma empresa de consultoria cujo objetivo é criar conhecimento por meio de pesquisas sobre tecnologias, execução de programas, consultoria, eventos e levantamento de soluções para que os seus clientes tomem decisões mais assertivas todos os dias.

Em seus documentos, o Gartner muitas vezes propõe definições e segmentações de mercado que permitem a comparação de soluções de acordo com suas funcionalidades e características. Nesse sentido, o Gartner propõe uma definição para o mercado de produtos DCAP (*Data-Centric Audit and Protection*) no documento "*Market Guide for Data-Centric Audit and Protection"*.

O DCAP é uma categoria de produtos caracterizados pela habilidade de monitorar de forma centralizada a atividade de usuários e administradores em relação a um conjunto específico de dados. Esta definição de mercado, segundo o Gartner, está composta por quatro segmentos que envolvem as principais funcionalidades associadas aos produtos para DCAP. São eles:

a) DAP (*Database Audit and Protection*): implementa políticas de segurança de dados, descoberta e classificação de dados, gerenciamento de acesso privilegiado, monitoramento de atividade de dados ou análise comportamental, proteção de dados e auditoria.

b) DAG (*Data Access Governance*): também pode ser conhecido como FCAP (*File-centric audit and protection*). Os produtos focam na implementação de políticas de segurança de dados, descoberta e classificação de dados, monitoramento de atividades, auditoria de repositório de arquivos e serviços de diretórios. São produtos muito próximos à abordagem de gerenciamento de acesso e identidade (IAM - *Identity Access Management*).

c) CASB (*Cloud Access Security Broker*): envolve ferramentas com funcionalidades de descoberta e classificação de dados, controle de acesso, monitoramento de atividade, auditoria e proteção através de bloqueio, criptografia, *tokenization* e quarentena, para aplicações e ambientes de armazenamento em nuvem.

d) DP (*Data Protection*): foca em proteção de dados utilizando criptografia, *tokenization* ou mascaramento de dados em diferentes tipos de repositórios de dados. Alguns produtos adicionam funcionalidades de alerta em tempo real , monitoramento de atividade e auditoria. Enquanto produtos DAP e DAG oferecem auditoria e monitoramento de acesso a dados em arquivos ou em bases de dados, os produtos DP focam somente em tipos de dados sensíveis.

A cada dia, mais empresas oferecem produtos DCAP que buscam cobrir mais divisões e mais tipos de repositório de dados, enquanto que outras empresas continuam a oferecer produtos que limitam sua cobertura a um ou dois tipos de repositório de dados. Cada vez mais produtos adicionam novas funcionalidades. As empresas fabricantes de produtos DCAP buscam oferecer plataformas de gerenciamento centralizado que permitem controlar políticas de segurança de dados entre os diversos tipos de repositórios de dados, sejam eles *on-premisses* ou na nuvem.

Considerando o cenário de produtos DCAP, muitas empresas tem desenvolvido funcionalidades comuns para descoberta e classificação de dados, gerenciamento e monitoramento de acesso, relatórios de auditoria e para prover alguma forma proteção. Contudo, estas funcionalidades não são criadas de forma homogênea e, sempre que uma solução é avaliada, cuidados devem ser tomados para garantir a escolha de produtos que atendam apropriadamente requisitos de controle e políticas de governança da organização. A seguir são apresentadas algumas das funcionalidades e pontos a serem avaliados em relação a cada uma delas:

- **Descoberta e classificação de dados:** os produtos podem vir com dicionários pré-definidos ou algoritmos de busca adaptados a políticas de conformidade. A capacidade de busca pode variar entre os produtos de acordo com a velocidade ou a performance no tratamento de falso-positivos. Além disso, cada ferramenta terá capacidade distinta de analisar arquivos não estruturados, ou metadados de arquivos, ou arquivos criptografados, ou várias outras características do dado que será classificado.
- **Gerenciamento de política de segurança de dados:** pode ser realizada via uma interface única de gerenciamento ou por múltiplas interfaces, de acordo com a funcionalidade de cada ferramenta. A aplicação da política é normalmente realizada de acordo com a identidade do usuário, por regras de negócio, ou pela utilização de grupos para ajudar a definir o acesso.
- **Monitoramento de privilégio de usuários e atividade de acesso a dados:** políticas de segurança são especificadas para o gerenciamento e monitoramento de privilégios de usuários das aplicações e de administradores. É importante monitorar mudanças em grupos do AD ou em privilégios individuais para garantir a correspondência correta com os requisitos das regras de negócio. A habilidade em detectar mudanças e criar alertas para uso de privilégios ou para alterações nos dados é importante para detectar atividades maliciosas internas ou externas, além de atender certos níveis de conformidade. Nem todos os produtos operam em nível de armazenamento, assim eles podem não oferecer a habilidade de avaliar usuários com alto privilégio como administradores de banco de dados, administradores de sistemas ou desenvolvedores. É importante avaliar se os produtos demonstram capacidade de operação contínua durante alta carga de processamentos nos servidores ou em casos de alto uso de rede. Se um monitoramento intensivo é necessário, alto uso da rede ou alta carga nos servidores pode levar a falhas no monitoramento.
- **Auditoria e relatório:** a necessidade de extrair relatórios cresce em uma organização juntamente com a maior necessidade de análise de dados. A auditoria em ambientes regulados pode requerer a necessidade de produzir informações relevantes sobre a atividade de usuários ao longo do tempo, o que necessitaria do acesso aos dados de pelo menos um mês. A conformidade da informação requer uma trilha de auditoria com várias capacidades de monitoramento, assim como comportamento anormal de usuários, mudanças nos dados, violações de política e mudanças de privilégios. No caso de um incidente de segurança, é importante a capacidade de utilizar os dados de log para investigar todas as atividades, incluindo acesso, alterações nos dados e privilégios.
- **Análise de comportamento, alerta e bloqueio:** a habilidade de configurar alertas de segurança com base em critérios predefinidos de monitoramento é crítica, e pode resultar em diferentes níveis de alertas relacionados a violações de política ou comportamentos suspeitos no acesso aos dados. Mecanismos de alerta incluem avisos na interface ou mensagens automáticas para equipes específicas, proprietários dos dados ou equipes do negócio. Funcionalidades adicionais incluem bloqueio automático do processo, acesso ou remoção de privilégios. Respostas rápidas e enérgicas podem incluir a remoção do acesso em casos, por exemplo, de downloads de grande quantidade de dados. Alguns produtos podem inclusive correlacionar regras para detectar comportamentos anormais. A capacidade de analisar tendência de acessos históricos provê melhor compreensão para a detecção de comportamentos inapropriados. Os produtos variam em relação à facilidade de uso da interface de gerenciamento e dos relatórios de segurança, e em relação à especificidade dos relatórios das diferentes plataformas de armazenamento de dados.
- **Proteção de dados:** algumas empresas oferecem ferramentas de proteção de dados utilizando criptografia, *tokenization* e mascaramento de dados, enquanto outras não oferecem qualquer ferramenta e requereriam a compra de outro produto separado. Em qualquer dos casos, esse tipo de ferramenta pode não estar integrada em uma única interface de gerenciamento. A seleção de ferramentas para esse tipo de funcionalidade irá requerer a avaliação das ameaças e dos riscos que cada uma irá oferecer. Por exemplo, a implementação de criptografia transparente em nível de base de dados previne o acesso por administradores do sistema, mas administradores da base de dados continuarão com acesso. Aplicar o mascaramento de dados por agentes no servidor de banco de dados pode prevenir o acesso pelos administradores da base de dados. A criptografia ou *tokenization* podem proteger os dados no momento de utilização ou em repouso na memória, mas deve se ter cuidado para não afetar o funcionamento das aplicações.

O mercado de produtos DCAP é caracterizado por empresas com estratégias cobrindo sistemas de gerenciamento de banco de dados (SGBDs), armazenamento não estruturado de arquivos (servidores de arquivos), ambientes parcialmente estruturados (*Sharepoint*, *NoSQL*, *MongoDB* and *Hadoop*), e serviços em nuvem. Algumas empresas inovadoras em proteção de dados estão desenvolvendo interfaces centralizadas de gerenciamento para os diversos tipos de repositórios de informação, mas nenhuma empresa consegue oferecer produtos para todas as funcionalidades do mercado DCAP.

Considerando as necessidades de negócio e os requisitos tecnológicos elencados no tópico 3 deste estudo, devem ser avaliadas ferramentas de auditoria para *Active Directory*, servidores de arquivos Windows e serviço de correio eletrônico que utiliza o *Microsoft Exchange*. Comparando as necessidades descritas no tópico 3 com as funcionalidades que o Gartner recomenda para comparação de ferramentas DCAP, é possível identificar como necessidade da Agência as seguintes funcionalidades:

Funcionalidades de produtos DCAP	Requisito de Negócio	Requisito Tecnológico
Descoberta e classificação de dados	4	3.2.2 - 18
Gerenciamento de política de segurança de dados	Não há	Não há
Monitoramento de privilégio de usuários e atividade de acesso a dados	2, 11, 14	3.2.2. - 5, 6, 7, 8, 9, 10, 20
Auditoria e relatório	9, 10, 12	3.2.2 - 3, 4, 14, 17, 19, 35
Análise de comportamento, alerta e bloqueio	5, 13	3.2.2 - 11, 12, 13
Proteção de dados	Não há.	Não há

A análise da tabela acima permite identificar que as necessidades de negócio e os requisitos tecnológicos poderiam ser atendidos com produtos que possuíssem o grupo de funcionalidades de descoberta e classificação de dados, monitoramento de privilégio de usuários, atividade de acesso a dados, auditoria, relatório, análise de comportamento, alerta e bloqueio. As ferramentas devem atender a essas funcionalidades para repositórios de arquivos, *Active Directory e Exchange*.

Em comparativo apresentado pelo Gartner no documento "*Market Guide for Data-Centric Audit and Protection*", empresas como IBM e Varonis poderiam fornecer ferramentas que atenderiam as funcionalidades acima relacionadas a repositório de arquivos. Quando se analisa a lista de empresas sem considerar a funcionalidade de análise de comportamento, alerta e bloqueio, seria possível adicionar à lista, uma quantidade maior de empresas.

O documento do Gartner está relacionado a ferramentas que forneçam funcionalidades para armazenamento de arquivos em servidores de arquivos, mas não relaciona ferramentas que atendem a necessidades para o ambiente de *Active Directory* e *Exchange*. Quando se inclui ferramentas para os três tipos de produtos, a lista fica mais restrita.

Em pesquisas realizadas na internet e considerando também empresas relacionada nos documentos do Gartner, foi possível localizar as ferramentas apresentadas a seguir. Elas serão analisadas quanto à capacidade de atender a necessidade da Agência, suas funcionalidades, a possibilidade de aquisição pelo governo, entre outros critérios. A lista de fabricantes e ferramentas apresentada abaixo inclui as fabricantes ou parceiros com as quais foi possível realizar contato por haverem respondido a solicitações via e-mail ou através do site do fabricante no período entre agosto e outubro de 2018. Algumas ferramentas já fornecidas para a Administração Pública, conforme apresentado no tópico 4.1, não aparecem na lista pois não foi possível contato com o fabricante ou algum parceiro. Por outro lado, estão na lista ferramentas e fabricantes de excelente qualidade que ainda não possuem contrato com a administração.

Não foi possível obter retorno de parceiros ou das fabricantes *CionSystems*, *Quest*, *NetIQ, Visual Click* e *NetAdmin*. Em alguns casos, foi feito contato com o fabricante ou o fornecedor, porém não obtivemos retorno com proposta de preços. Por outro lado, obtivemos retorno, incluindo proposta, dos fabricantes *Manage Engine*, *StealthBITS*, *Varonis*, *Netwrix* e *SailPoint*.

Fabricante	**Manage Engine**
Ferramentas	1. AD Audit Plus 2. AD Manager Plus 3. Exchange Reporter Plus 4. Recovery Manager Plus 5. AD 360
Descrição da solução e funcionalidades	A *Manage Engine* é uma divisão de gerenciamento de TI da corporação *Zoho.* Ela possui sistemas compreensivos de gerenciamento de TI que fazem o trabalho ficar mais simples e possui mais de 90 produtos e ferramentas. Eles fornecem soluções integradas para otimizar a TI, que incluem gerenciamento de dispositivos ou redes, segurança e sistemas de gerenciamento de usuário. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Agência. 1. AD Audit Plus: • Permite monitorar e visualizar mudanças no ambiente de servidores *Windows*, incluindo serviços como *Active Directory*, estações de trabalho, servidores de arquivos e servidores do domínio. • Monitora qualquer servidor Windows apresentando relatório de eventos, eventos de sistema ou de tarefas agendadas, ou quaisquer mudanças de políticas e processos. • *Active Directory*: administradores podem avaliar todos os eventos do domínio, como logon e logoff, auditoria de usuários, grupos, computadores, políticas de grupo (GPO), mudanças em unidades organizacionais (OUs) com a utilização de alertas por e-mail ou dezenas de relatórios predefinidos na ferramenta. • Mantem registros de alterações em diversos objetos do AD, como *conteiner*, *contacts, schema, configuration, site, DNS* e permissões. • Servidores de arquivos: avalia de forma segura servidores de arquivos e *failover cluster* por mudanças em arquivos (criação, modificação ou deleção) e pastas. Permite auditoria de acesso, compartilhamentos e permissões. • Estações de trabalho: monitora todo *logon* ou *logoff* de usuário e as ações dos usuários no dia a dia com relatórios detalhados de eventos de *logon* bem sucedidos ou com falha em estações da rede. • Provê alertas instantâneos na própria aplicação e em alertas por e-mail. • Permite configuração de alertas com base em limites que auxiliam de forma precisa a identificação de problemas. 2. AD Manager Plus: • É uma ferramenta web que permite gerenciar objetos no AD, caixas postais do Exchange, licenças do Office 365, Skype for Business e outras atividades em série. • Inclui funcionalidades de delegação para a central de atendimento de usuários, *workflow*, automação, entre outras tarefas de gerenciamento. • Permite provisionar de forma padronizada contas de Exchange ou Lync a partir de modelos pré-definidos. • Permite provisionar contas de usuários novos automaticamente e também arquivar as pastas e revogar permissões quando a conta é bloqueada. • Permite automatizar operações críticas ou rotineiras do AD. • Permite delegação de tarefas de gerenciamento de usuários a gerentes de negócio com a utilização. • Permite gerenciar caixas postais compartilhadas, de salas e de equipamentos. • Permite gerar relatórios pré-configurados diversos sobre AD e Exchange. • Permite a delegação de tarefas para os técnicos do serviço de atendimento de usuários dentro de OUs específicas. • Permite delegar tarefas como reconfiguração de senhas, criação de usuários, entre outras. • Permite delegar se a elevação de privilégio dos técnicos no AD. • Permite controlar a execução de tarefas automatizadas com o uso de *workflow* e automatização. • Permite automatizar tarefas rotineiras do AD, como limpeza do AD. • Permite configurar fluxos de trabalho com aprovação para a execução de tarefas no AD. 3. Exchange Reporter Plus :

	• Provê informações de componentes do Exchange, incluindo caixas de e-mail, OWA, listas de distribuição, pasta públicas e seus conteúdos. • Permite identificar caixas inativas ou órfãs e permite a remoção segura delas, além de informações detalhadas sobre cada caixa. • Relatório e análise de tráfego de e-mail entre caixas postais, listas de distribuição e pastas públicas. • Permite supervisionar acessos e políticas relacionadas a *ActiveSync*. • Permite configurar alarmes para detecção de eventos como mudança de permissões, problemas nas bases, *logon* de usuários não proprietários ou alterações em permissões "*send-as*". 4. Recovery Manager Plus: • Permite recuperação de objetos do AD, sem necessidade de parar ou reiniciar o serviço. • Permite automatização e agendamento de backup de AD. • Permite comparação de mudanças em atributos de objetos ao longo do tempo. • Permite restauração singular de objetos ou de seus atributos. 5. AD 360 • É uma solução para gerenciamento de acesso e identidade (IAM) que combina as funcionalidades das soluções de AD da *Manage Engine* em uma única interface e com *single sign-on.* A seguir são apresentados algumas informações adicionais em relação às soluções da Manage Engine: • Não instala agentes nos servidores monitorados e as informações são coletadas com base no log de eventos do Windows. • Em caso de perda de comunicação entre o servidor de auditoria e servidor monitorado, pode ocorrer perda de informação de auditoria, caso o servidor monitorado não mantenha os logs por período superior ao tempo de perda da comunicação. • Não realiza modificações no *schema* do *active directory* para integração com AD. • As ferramentas são licenciadas com base na quantidade de domínios a serem monitorados e na quantidade de técnicos que operam as ferramentas • A ferramenta não provê atuação proativa em casos de incidentes de segurança cibernética ou ataques de *malware*. • Não provê funcionalidade de alteração de múltiplos objetos em servidores de arquivos, ou automatização de tarefas para servidores de arquivos. • Não provê ferramenta ou funcionalidade para descoberta e classificação de dados. • Não provê ferramenta ou funcionalidade de análise comportamental dos usuários.

Fabricante	**Netwrix**
Ferramentas	1. *Netwrix Auditor* para *Active Directory* 2. *Netwrix Auditor para servidores de arquivos* 3. *Netwrix Auditor para Exchange.*
Descrição da solução e funcionalidades	A *Netwrix Corporation* é uma empresa focada exclusivamente em prover uma visão completa para segurança de dados e mitigação de riscos em ambientes híbridos. Com esse foco, eles oferecem em seus produtos funcionalidades mais robustas que ferramentas legadas de auditoria de mudanças. Segundo informações da empresa, centenas de milhares de departamentos de TI ao redor do mundo possuem *Netwrix Auditor* como solução de auditoria. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Agência. 1. *Netwrix Auditor* para *Active Directory* • A ferramenta provê uma visão completa do que está acontecendo no *Active Directory* e *Group Policy.* • Permite detectar todas as alterações do *Active Directory* e de *Group Policy.* • Provê detalhes de quem, o que, quando e onde uma alteração foi realizada, e os valores anteriores e posteriores à alteração. • Permite auditar *logon* com relatórios de tentativas de logon ou acesso a sistemas críticos. • Fornece histórico completo de logon de qualquer usuário. • Permite comparar o estado atual de usuários, grupos, suas permissões no AD, suas GPOs e suas configurações com um padrão preestabelecido. • Provê relatórios alinhados a controle de padrões internacionais de conformidade do ambiente. • Fornece relatório sobre alterações de configurações de políticas de grupo com detalhamento dos valores anteriores e posteriores à modificação. • Fornece alertas para desvio de padrões de comportamento em alterações do AD, tentativas repetitivas de logon e outras ameaças ao ambiente. • Possui ferramenta de pesquisa refinada sobre os dados auditados. • Fornece descoberta de comportamento anormal de usuários maliciosos e contas comprometidas pela agregação de suas atividades anormais no AD e em outros sistemas críticos. • Simplifica a detecção de possíveis ameaças ao AD, como logons não habituais que poderiam indicar o furto de uma credencial de acesso. • Auxilia na imposição do princípio de contas com baixo privilégio no ambiente. • Permite a recuperação de objetos e o retorno à configuração anterior. • Permite identificar usuários inativos, alertas de contas expiradas ou contas bloqueadas. • Permite a auditoria de mudanças e logons no AD sem necessidade de agente 2. *Netwrix Auditor* para servidores de arquivos

	• Facilita a governança de acesso a dados e um melhor gerenciamento dos dados através de maior visibilidade sobre a atividade em arquivos e do comportamento dos usuários. • Aumenta visibilidade sobre alterações ou acesso suspeito a dados, comportamento anômalo do usuário, direitos de acesso excessivos. • Fornece relatórios que mapeiam as mais comuns regulações de conformidade. • Permite detectar, investigar ou remediar proativamente alterações não necessárias, como deleções acidentais a dados críticos. • Permite a criação de alertas customizados para ameaças, como muitas alterações de arquivos ou tentativas de acesso. • Possui ferramenta de pesquisa refinada sobre os dados auditados. • Provê informação detalhada sobre alterações nos servidores de arquivos para detalhes como quem fez a alteração, o que foi alterado, quando e onde ocorreu a alteração. • Permite a comparação do estado atual e passado de permissões para alinhar com as regras organizacionais de acesso. • Permite a descoberta e classificação de dados sensíveis através da informação sobre que tipo de dados sensíveis a organização possui, onde está localizado, quem possui acesso ao dado e como ele é utilizado. • Alerta para a ocorrência de muitas alterações de arquivos ou tentativas de acesso em um curto período de tempo, o que permitiria responder a ataques *ransonware* ou atividades de usuários suspeitos. • Provê informação detalhada sobre o proprietário dos dados, o uso dos dados, o volume, os dados duplicados ou obsoletos . • Coleta as informações sem a utilização de agentes e, assim, não interfere no desempenho do sistema e seus processos. 3. *Netwrix Auditor* para *Exchange* • Auxilia na detecção e investigação de comportamento de usuários suspeitos. • Permite visualização de eventos críticos de acesso e mudanças, permitindo detecção de atividades suspeitas e rápida resposta. • Provê relatórios predefinidos de conformidade com padrões internacionais. • Ajuda a minimizar problemas de e-mails ao permitir aos administradores detectar problemas e identificar a causa raiz. • Permite identificar acesso de usuário não proprietário a caixa de e-mail, incluindo informações sobre quem acessou qual e-mail, quando e de onde foi acessado o e-mail. Além disso, permite identificar o conteúdo que foi lido, alterado, copiado ou deletado. • Possui ferramenta de pesquisa refinada para identificar a causa raiz e para ajudar a identificar como um evento de alteração ou acesso ocorreu. • Permite responder rapidamente a atividades suspeitas e prevenir proativamente o vazamento de dados com alertas customizados para determinados padrões de ameaça. • Notifica atividades suspeitas que podem comprometer a segurança de informações sensíveis ou a disponibilidade do serviço de e-mail. A seguir são apresentadas algumas informações adicionais em relação às soluções desta empresa: • Não instala agentes nos servidores monitorados e as informações são coletadas com base no log de eventos do *windows*. • Em caso de perda de comunicação entre o servidor de auditoria e servidor monitorado, pode ocorrer perda de informação de auditoria, caso o servidor monitorado não mantenha os logs por período superior ao tempo de perda da comunicação • Não realiza modificações no *schema* do *active directory* para integração com AD. • As ferramentas são licenciadas com base na quantidade de contas ativas de colaboradores no AD e de contas de serviço ou sistema ativas no AD. • As ferramentas desta empresa são focadas exclusivamente em auditoria e, assim, não fornecem funcionalidade para administração do AD, servidores de arquivos ou Exchange. Também não fornecem funcionalidades para ações proativas em casos de incidentes de segurança cibernética e ataques de *malwares*. • As ferramentas possuem funcionalidade para descoberta e classificação de dados. • As ferramentas possuem funcionalidade de análise comportamental dos usuários.

Fabricante	**Varonis**
Ferramentas	1. Varonis DatAdvantage para Directory Services 2. Varonis DatAdvantage para Windows 3. Varonis DatAdvantage para Exchange 4. Varonis DataPrivilege 5. Varonis IDU Classification Framework 6. Varonis DataAlert 7. Varonis Data Governance Suite
Descrição da solução e funcionalidades	A Varonis é uma empresa pioneira em segurança e análise de dados, especializada em segurança, governança, conformidade, classificação e análise de dados. Suas ferramentas permitem detectar ameaças internas e ataques cibernéticos pela análise da atividade sobre arquivos e análise do comportamento do usuário. Também é possível a prevenção de desastres, o bloqueio de dados sensíveis e a sustentação de um estado seguro dos dados com automação. As soluções da empresa aproveitam metadados para que as organizações possam, de maneira inteligente, acessar, governar, migrar e dispor de seus dados não-estruturados. Baseadas em uma tecnologia patenteada e em ferramentas de análise precisa, as soluções fornecem às organizações total visibilidade e controle dos seus dados, garantindo que somente os usuários corretos tenham acesso aos dados corretos. Todo o uso é monitorado, e o abuso, assinalado. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam

associadas às necessidades da Agência.

1. *Varonis DatAdvantage* para *Directory Services*

- É construído para apresentar, filtrar e analisar estruturas hierárquicas grandes e complexas, estendendo as capacidades das ferramentas de administração padrão.
- Permite auditar quem fez alterações no Active Directory, e quando elas foram realizadas.
- Fornece uma trilha de auditoria que inclui alterações em grupos, OUs e políticas de grupo (GPO) para qualquer período de tempo.
- Permite auditar as alterações de configuração, as mudanças recentes em políticas de senhas, quem realizou e de qual computador foram realizadas a mudança nas políticas de grupo (GPOs) do AD.
- Fornece recomendações para grupos não utilizados e associações a grupos.
- Permite identificar associações de grupo excessivas para uma remoção segura e sem afetar o processo de negócio.
- Permite modelar alterações sem afetar o ambiente de produção.
- Permite visualizar a hierarquia de serviços de diretórios pela ferramenta DatAdvantage GUI.
- Permite visualizar domínios, OUs, computadores, grupos e outros objetos de domínio pela ferramenta DatAdvantage GUI.
- Permite gerar alertas em tempo real para eventos de interesse, com a ferramenta *Varonis DatAlert*
- Ferramenta pode ser estendida com a funcionalidade de classificação de dados com a ferramenta *IDU Classification Framework*.
- Usuários de negócio e proprietários de dados podem ser envolvidos diretamente com a ferramenta DataPrivilege.

2. *Varonis DatAdvantage* para *Windows*

- É uma solução que agrega informações de eventos sobre usuários, permissões, dados e acessos a diretórios e servidores de arquivos.
- A informação coletada é analisada para fornecer informações detalhadas de uso e determinar o acesso correto baseado em um necessidade de negócio.
- Permite visibilidade completa sobre a estrutura de permissões dos servidores Windows.
- Mostra os dados acessíveis a cada usuário ou grupo, assim como usuários e grupos com permissões a uma pasta.
- Identifica pastas que necessitam de um proprietário.
- Fornece uma trilha de auditoria de cada arquivo dos servidores monitorados.
- Permite pesquisa rápida sobre os dados normalizados, processados e armazenados.
- Realiza a coleta de informações de auditoria com o mínimo impacto para os servidores de arquivos e sem a necessidade de habilitar a auditoria nativa do Windows.
- Permite identificar permissões não necessárias em grupos e em arquivos para uma remoção segura e sem afetar o processo de negócio.
- Realiza alterações em objetos do AD e ACLs em uma interface única.
- Identifica os proprietários de negócio dos dados pela análise estatística da atividade dos usuários.
- Gera relatórios automatizados e personalizados para envolver proprietários dos dados no processo de governança de dados.
- Ferramenta pode ser estendida com a funcionalidade de classificação de dados com a ferramenta *IDU Classification Framework*.
- Permite gerar alertas em tempo real para eventos de interesse com a ferramenta *Varonis DatAlert.*
- Permite identificar mudanças em membros de grupos e em permissões.
- Permite modelar e simular mudanças em permissões sem afetar o ambiente de produção.

3. *Varonis DatAdvantage* para *Exchange*

- É uma solução que agrega informações de eventos sobre usuários, permissões, dados e acessos a caixas de e-mail e pastas públicas do Exchange.
- A informação coletada é analisada para fornecer informações detalhadas de uso e determinar o acesso correto baseado em um necessidade de negócio.
- Permite visibilidade completa sobre as permissões no Exchange.
- Fornece uma trilha de auditoria para toda atividade de e-mail.
- Permite detectar picos de uso repentino na atividade de e-mail.
- Fornece recomendações para remoção de excesso de permissões e modelagem de mudanças.
- Identifica os proprietários do dados de negócio pela análise estatística da atividade dos usuários.
- Mostra os dados acessíveis a cada usuário ou grupo no ambiente de e-mail, assim como toda caixa postal ou pasta pública que pode ser acessada por um usuário ou grupo.
- Identifica e ajuda a corrigir excesso de permissões de acesso aos recursos.
- Monitora qualquer evento de e-mail e mudança de permissões no ambiente do Exchange.
- Permite pesquisa rápida sobre os dados normalizados, processados e armazenados.
- Realiza a coleta de informações de auditoria com o mínimo impacto para os servidores monitorados.
- Realiza a análise da atividade no ambiente de e-mail em busca de atividades anormais, como *worms,* vírus e *spam.*
- Permite remover com segurança associações de grupo excessivas sem afetar o processo de negócio, através da combinação de informação sobre quem pode acessar um dado e a trilha de auditoria de quem o está acessando.
- Permite modelar e simular mudanças em permissões sem afetar o ambiente de produção.
- Identifica os proprietários de negócio dos dados pela análise estatística da atividade dos usuários.
- Relatórios sobre o acesso aos dados, a atividade, as mudanças em pastas e grupos, e os dados obsoletos podem ser providos automaticamente aos proprietários dos dados.

4. *Varonis DataPrivilege*

- É uma ferramenta que permite dar aos usuários do negócio o poder de revisar e gerenciar o controle de

acesso a pastas, arquivos ou grupos de segurança sem a assistência da TI e sem necessidade de direitos administrativos.
- Permite garantir que o acesso a grupos, listas de distribuição e dados sensíveis de negócio seja revisado constantemente pelas pessoas certas.
- Algoritmos de aprendizado marcam os usuários que não deveriam mais ter acesso, facilitando a revisão dos acessos.
- Fluxos de autorização permitem aos usuários requisitar acesso por uma interface web. Cada requisição é direcionada ao proprietário correto baseado em fluxos pré-definidos.
- A resposta a requisições de acesso pode ser dada com a resposta a um e-mail.
- Após a aprovação de uma requisição de acesso, o acesso é garantido pela ferramenta *DataPrivilege* sem o envolvimento da TI.
- Permite atribuir data de validade a uma autorização e garantir que seja revogada automaticamente.
- Permite automatizar acesso ou revogar acesso baseado em atributos dos usuários.
- Permite auditar todas as alterações.
- Autorizações, revisões de direitos e outros relatórios gerenciais fornecem evidências da aderência ao processo e ajudam a atender a requisitos de conformidade.
- O processo de revisão de acesso, geração de relatórios e modificações é feito diretamente via navegador web.
- Permite configurar agendamentos para revisões de direitos de acesso com base em departamento, em informações sensíveis, ou outros tipos de informação.

5. *Varonis IDU Classification Framework*

- Permite visualizar onde os dados mais sensíveis para a organização estão armazenados.
- Permite recomendar como o acesso ao dado sensível pode ser reduzido.
- Permite classificar dados sensíveis com base em expressões regulares, padrões pré-definidos de conteúdo ou busca por conteúdo baseada em dicionário, incluindo auto atualização de dicionários.
- Permite busca incremental para os novos dados criados ou modificados e não necessita de uma busca completa a cada nova verificação.
- Permite criar regras de classificação baseadas em conteúdo e em metadados.
- Permite criar buscas por palavras chave em arquivos, metadados de arquivos, frases ou expressões regulares.
- Fornece resultados de classificação precisos por usar algoritmos de verificação, como IBAM, Luhn e Verhoeff.
- Permite coletar metadados sobre usuários e grupos, permissões de quem pode acessar um dado e a atividade de quem está acessando o dado, para fornecer informações eficientes sobre a atividades realizadas sobre a informações.
- Permite obter alertas em tempo real para eventos de interesse, como arquivos sensíveis que foram deletados ou modificados com a ferramenta *Varonis DatAlert*.
- Permite incorporar a informação de classificação de conteúdo produzida pelo motor de classificação de conteúdo da Varonis ou por um fonte externa de classificação de metadados, como RSA DLP.

6. *Varonis DataAlert*

- É um sistema que permite detectar e alertar sobre atividades suspeitas em sistemas de arquivos e e-mail.
- Permite monitorar ativos críticos em busca de atividades suspeitas ou comportamento anormal de usuários.
- Permite monitorar eventos em plataformas Windows, Unix/Linux, NAS, AD, Sharepoint ou Exchange.
- Permite detectar falhas potenciais de segurança, falhas de configuração ou outros problemas.
- Permite a redução do tempo total necessário para detectar e corrigir problemas nos ativos.
- Permite detectar ameaças com a utilização de modelos preditivos de ameaças com base em análise avançada, comportamento do usuário e aprendizado automático de maquina.
- Permite a defesa contra ameaças internas, códigos maliciosos como *ransonware*, e violações de dados.
- Possui um painel web que permite pontuar, triar, analisar, priorizar alertas e tomar ações para resolução de incidentes.
- Permite implementar ações personalizadas com a execução de linhas de comando.
- Pode ser integrado com SIEM e soluções de gerenciamento de redes.
- Por detrás dos modelos de ameaças baseadas no comportamento dos usuários, há uma equipe de especialistas em segurança e cientistas de dados trabalhando continuamente.

7. *Varonis Data Governance Suite*

- É uma solução para governança de dados que se utiliza de uma estrutura de dados extensível e escalável para prover inteligência organizacional sobre seus dados.
- É uma solução que está integra as outras soluções como *DatAdvantage*, *DataPrivilege* e *IDU Classification Framework*.
- Permite automatizar o processo de revisão e autorização de acessos.
- Permite a aplicação de políticas nos dados de infraestrutura e garantir conformidade regulatória.
- Permite a aplicação automática de aprovações e revogações de acessos aos arquivos.
- Fornece uma trilha de auditoria para todo evento de acesso.
- Permite a identificação de acessos excedentes para removê-los e fornece a possibilidade de simular alterações sem afetar o ambiente de produção.
- Permite classificar dados sensíveis ou críticos ao negócio de forma precisa e rápida.

Fabricante	**StealthBits**

Ferramentas	1. *StealthAUDIT for Active Directory* 2. *StealthAUDIT for File Systems* 3. *StealthAUDIT for Exchange* 4. *StealthBits Sensitive Data Discovery and Classification* 5. *StealthAUDIT Action Modules* 6. *StealthINTERCEPT*
Descrição da solução e funcionalidades	A *STEALTHbits Technologies Inc.* é uma companhia de sistemas de segurança cibernética focada na proteção dos dados sensíveis e na proteção contra credenciais roubadas para ataque aos dados das organizações. A empresa permite às organizações reduzir o risco de segurança, atender a requisitos de conformidade e diminuir os custos de suas operações pela remoção de acessos inapropriados, pela aplicação de políticas de segurança e pela detecção de ameaças avançadas. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Agência. 1. *StealthAUDIT for Active Directory* • É um modelo estruturado para auditoria, conformidade legal e normativa, e governança que provê coleta de dados, análise, recuperação e relatórios para combater os desafios de complexidade, segurança e gerenciamento enfrentados pelas organizações. • Não utiliza agentes para execução de suas funções. Por isso, possui coleta rápida e com pouca carga sobre os sistemas. • Possui dezenas de relatórios pré-configurados e permite a criação de relatórios personalizados rapidamente. • Permite a configuração de fluxos de trabalho alinhados a segurança, conformidade legal e gerenciamento operacional. • Coleta informações de objetos e seus atributos, políticas de grupo (GPOs), configurações, membros de grupos, domínios, *sites,* relações de confiança, ou qualquer informação do AD. • Permite identificar e configurar proprietários de grupos. • Permite automatizar a revisão de associações a grupos. • Permite descentralizar (*self-service*) o gerenciamento de grupos e requisições de associações a grupos. • Realiza coleta, inventário e análises sobre permissões a todos os objetos e permite compreender quem possui acesso privilegiado no *Active Directory* (AD). • Verificações pré-configuradas e personalizáveis de boas práticas de segurança permitem identificar proativamente configurações críticas de segurança que deixam o AD vulneráreis a ataques. • Permite identificar objetos obsoletos, duplicados ou problemáticos e limpá-los de forma automatizada. • Permite automatizar a produção de artefatos de conformidade pelo fornecimento de relatórios pré-configurados e personalizáveis alinhados a vários padrões de conformidade, como HIPAA, PCI-DSS, GDPR e SOX. 2. StealthAUDIT for File Systems • É uma ferramenta que permite à organização satisfazer requisitos de conformidade legal e reduzir seu risco de exposição através do controle completo e automatizado de governança de acesso a dados não estruturados residentes em servidores de arquivos. • Permite reduzir o risco de ameaças internas, perda de dados sensíveis e condições não desejadas de acesso livre em servidores de arquivos. • Provê um fluxo automatizado para identificação de proprietários dos dados. • Permite confirmar a correta propriedade de um dado. • Reúne detalhes completos de permissões de acesso a compartilhamentos, pastas e arquivos e permite identificar condições anormais como quebra de herança, SIDs com problema, permissões diretas de usuários e acesso amplo permitido. • Correlaciona informação do AD com informação coletada nos compartilhamentos para determinar como um usuário pode acessar um recurso e também o nível de permissão do usuário. • Coleta metadados de arquivos para compreender tudo o que é necessário sobre um arquivo, incluindo tipo, atributos, proprietários e outros rótulos. • Permite identificar o proprietário mais provável de um compartilhamento ou pasta, incluindo gerentes comuns, criadores de conteúdos e usuários mais ativos. • Monitora atividade em sistemas de arquivos NAS e Windows para uma visão completa de quais arquivos, pastas ou compartilhamentos os usuários estão acessando, assim como o que eles fazem com os dados. • Permite identificar onde os dados sensíveis estão armazenados para entender onde o risco de acesso existe e poder fortalecer as iniciativas de prevenção de perda de dados. • Permite rotular automaticamente arquivos com suas classificações necessárias. • Fornece suporte a sistemas de arquivos locais ou em nuvem. • Permite coletar apenas informações necessárias à auditoria através de um escopo granular e flexível, e de um controle dos eventos monitorados. • Identifica e movimenta automaticamente dados obsoletos ou dados sensíveis em casos de necessidade de redução de custos de armazenamento e diminuição de riscos aos dados. 3. *StealthAUDIT for Exchange* • É uma ferramenta que provê uma visão profunda do Exchange local ou Online, pela combinação da coleta, análise e readequação dos dados. • Fornece uma visão ampla sobre como o acesso está ou foi provisionado no Exchange. • Provê uma visão global sobre caixas de e-mail, pastas públicas, membros de listas de distribuição e PSTs, que inclui detalhes específicos do tipo de acesso garantido a cada usuário. • Permite aos administradores obter métricas de uso do sistema de e-mail, com a compreensão de quem usa o que, a frequência de utilização, ou se os recursos são ainda necessários. • Permite diminuir os riscos de segurança e os eventos de vazamentos de informações.

	• Permite reduzir o número de recursos não necessários ou obsoletos. • Permite reduzir os custos do atendimento de serviços pela resolução de pequenos problemas proativamente. • Permite otimizar o desempenho pela diminuição do impacto de usuários poderosos na infraestrutura crítica. • Permite auditar o acesso de um não proprietário a uma caixa de e-mail. 4. *StealthBits Sensitive Data Discovery and Classification* • Fornece às organizações a habilidade de procurar por mais de 400 tipos de conteúdos, que incluem imagens, informação sensível, números sociais e dezenas de outros tipos de informações sociais. • Permite a criação de critérios únicos a cada organização, como número de identificação de empregados, chaves de segurança, formulas de produtos ou outros tipos. • Permite coletar metadados de arquivos, incluindo rótulos aplicados por processo internos da organização ou outra ferramenta, assim como aplicar rótulos que identificam o nível de sensibilidade do arquivo, conteúdo ou outra designação. • Permite gerar relatórios pré-configurados ou personalizados que podem ser rotulados para fácil identificação. • Permite a revisão dos dados encontrados no ambiente pelos responsáveis, a marcação de falsos positivos e a inspeção de arquivos com informação sensível. 5. *StealthAUDIT Action Modules* • Permite aos usuários readequar diversas condições identificadas durante o processo de coleta e análise em série de dados, assim como organizar fluxos de trabalho para automatizar processos manuais ou procedimentos associados ao AD, servidores de arquivos, Sharepoint, Exchange ou outras ferramentas. • Os módulos de ação são habilitados dentro do StealthAUDIT e existem para os serviços de AD, sistemas de arquivos, caixas postais do Exchange, entre outros. • O módulo de ação para AD fornece operações como histórico de limpeza e configuração de SID; mudanças de detalhes ou atributos de objetos de computadores; criação de usuários; remoção de objetos de usuário, grupos ou computadores; desativação ou habilitação de usuários; modificação de membros de grupos; movimentação de objetos; configuração ou reconfiguração de senhas de usuários; ou desbloqueio de usuários. • O módulo de ação para AD permite, por exemplo, automatizar processos de negócio como desativação de contas de rede após a saída de um colaborador, limpeza de objetos obsoletos ou não necessários, ou sincronização de atributos de objetos com sistemas de HR. • O módulo de ação para sistemas de arquivos fornece operações como alterações de atributos; alterações de permissões e auditoria; alteração em permissões de herança; alteração em permissões de compartilhamento; cópia de arquivos; execução de processos remotos; movimentação de arquivos; remoção de permissões; remoção de permissões compartilhadas; e alterações de nomes. • O módulo de ação para sistemas de arquivos permite automatizar funções do ciclo de vida dos dados, permitindo localizar arquivos obsoletos ou não utilizados, movimentá-los para tipos de armazenamento menos custosos ou remover os dados em série, de acordo com a necessidade que se deseja implementar. Esse módulo também poderia ser utilizado para a marcação de arquivos ou a gravação de atributos que permitiriam iniciativas para prevenção da perda de dados, *business intelligence* (BI) ou classificação dos dados. • O módulo de ação para caixas de e-mail fornece operações como remoção de conteúdos em caixas de correio; alterações em permissões; remoção de permissões; delegação de caixas de e-mail; remoção de delegações; e remoção de SIDs obsoletos. • O módulo de ação para caixas de e-mail permitiria, por exemplo, remediar acessos privilegiados a caixas de e-mail, com a remoção de permissões de contas administrativas que não deveriam mais ter permissão e com a diminuição da exposição inapropriada de dados. 6. StealthINTERCEPT • É uma solução de monitoramento em tempo real de acesso e alterações realizada no AD, sistemas de arquivos e Exchange. • É capaz de identificar ataques a sistemas de arquivos ou ataques baseados em autenticação, monitorar o uso e o abuso de contas privilegiadas, e detectar alterações críticas realizadas no ambiente. • É capaz de iniciar um controle preventivo que bloqueia os ativos críticos e força políticas de escrita. • Previne mudanças e atividades que põe em risco a organização • Protege objetos críticos de alterações ou acessos não autorizadas e previne abuso de credenciais. • Automatiza a geração de artefatos de conformidade críticos alinhados a padrões regulatórios da indústria. • Correlaciona dados de ameaça fornecendo informações sobre técnicas de ataque e comportamento, sem a necessidade dos logs nativos do sistema operacional. • Monitora mudanças, acessos ou consultas a objetos críticos, e tentativas de comprometimento de credenciais. • Detalhes compreensíveis para cada evento melhoram a visibilidades e tornam os dados mais utilizáveis. • Alerta qualquer destino sobre eventos críticos em tempo real em níveis globais ou de acordo com políticas específicas. • Permite execução de ações avançadas usando automação simples e funcionalidades de scripts.

Fabricante	**SailPoint**
Ferramentas	1. *SecurityIQ for Active Directory* 2. *SecurityIQ for Windows and Unix File Shares* 3. *SecurityIQ for Exchange*

Descrição da solução e funcionalidades	A *Sailpoint* é uma empresa fundada em 2005 que provê soluções inovadoras para problemas de negócio e um ambiente de trabalho colaborativo relacionado a identidades. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Agência. 1. *SecurityIQ for Active Directory* • É uma ferramenta que permite proteger efetivamente o AD e que provê uma visão completa sobre usuários, grupos, recursos e qualquer atividade associada a eles. • Permite prover uma prova de conformidade durante auditorias e reduzir o tempo gasto em análises forenses. • Permite monitorar e responder a atividades em tempo real • Permite ampliar a estratégia de gerenciamento de identidades de acesso (IAM - *Identity Access Management*) e prover uma governança de acessos ampla a dados não estruturados. • Permite identificar e limpar contas obsoletas, automatizar requisitos de auditoria e agilizar revisões e requisições de acessos, que permitem reduzir a carga de trabalho da área de tecnologia. • Provê monitoramento de atividades baseado em um contexto de segurança, que permite identificar e responder a violações rapidamente. • Permite monitorar ações como criação, remoção, recuperação, movimentação, alteração de atributos, e adição e remoção de permissões a objetos. • Permite auditar alterações de políticas. • Permite monitorar alterações na regra FSMO (*Flexible Single-Master Operation*) do AD. • Permite monitorar alterações nas políticas de domínio. • Permite monitorar bloqueio de contas, reconfigurações de senha e logons de conta de rede. • Permite monitorar ações como modificação de situação; modificação de filtros de segurança; modificação de propriedades; modificação, adição, modificação ou remoção de links; e histórico de alterações sobre objetos de política de grupos (GPO). • Permite a execução de ações em tempo real com base nas atividades monitoradas para o tratamento de comportamentos arriscados. • Permite o envio de alertas em tempo real por e-mail, assim como execução de ações remotas como verificação ou modificação de acessos. • Permite enviar ou receber alertas para a tomada de ações de governança como notificações, suspensões de contas ou outras. • Realiza coleta e análise automática de todos os direitos em ambientes do *Active Directory* • Permite identificar quem possui acesso a qual dado. • Permite identificar violações de gerenciamento de acesso ou práticas ruins de gerenciamento. • Auxiliar na correção de problemas de governança como combinações não recomendadas de grupos de permissões ou remoção de grupos cíclicos. • Permite aos proprietários dos dados ter visibilidade sobre os dados que possuem, configurar alertas, fornecer acesso controlado por meio de solicitações de acesso com autoatendimento, ou adicionar e remover acessos de alto risco de forma automática. 2. *SecurityIQ for File Shares* • É uma ferramenta que permite estender controles de governança de identidades a dados sensíveis armazenados em arquivos. • Permite descobrir dados sensíveis expostos espalhados entre uma diversidade de compartilhamentos de arquivos. • Permite identificar, classificar e dar segurança a dados sensíveis armazenados em repositórios locais ou na nuvem, de acordo com regulações como GDPR e HIPAA. • Permite coletar e analisar automaticamente permissões de acesso ou modificação em arquivos. A partir disso, é possível corrigir problemas de acesso para melhorar a segurança dos dados. • Ajuda a identificar e escolher proprietários para os dados. • Painéis práticos alertam os proprietários dos dados sobre riscos de exposição a serem corrigidos, e permitem gerenciar as requisições e revisões de acesso aos dados. • Além de permitir responder quem possui acesso a qual dado, permite revelar dados expostos e outras violações ou práticas ruins de gerenciamento de acesso. 3. *SecurityIQ for Exchange* • É uma ferramenta que permite ter uma compreensão completa das atividades e modelos de permissão do Microsoft Exchange, além de não afetar a performance do ambiente protegido. • Determina quem tem acesso ao dado, como o dado é utilizado e aplica controles em tempo real para dar segurança ao dado. • Provê uma prova de conformidade durante auditorias e reduz o tempo gasto em análises forenses. • Amplia a estratégia de governança de identidades de acesso provendo governança de acesso aos dados não estruturados. • Identifica dados e contas obsoletas. • Automatiza requisitos de auditoria. • Agiliza a revisão de acessos. • Reduz a carga de trabalho da área de TI. • Fornece monitoramento ativo baseado em contexto com alertas em tempo real. • Toda atividade monitorada é enriquecida com um contexto completo de segurança de sistemas de segurança como Ad. O contexto completo é importante para identificar violações e responder rapidamente, além de auxiliar em análises forenses. • Coleta e analisa todos os direitos concedidos a colaboradores ou em pastas públicas, incluindo permissões "*Send As*" e "*Send on Behalf*". • Permite identificar dados expostos. • Permite a escolha dos proprietários dos dados e provê um conjunto de painéis que fornecem inteligência sobre os dados que os proprietários possuem. • A ferramenta cobre tanto Exchange local quanto Exchange Online dentro da mesma licença, suportando assim arquiteturas híbridas do Exchange.

	• Simplifica solicitações de acesso e gerencia revisões periódicas e revisões baseadas em acesso. • Automatiza o provisionamento e a revogação de acessos.

Os fabricantes e as ferramentas apresentadas nos quadros acima mostram que existem diversos tipos de ferramentas disponíveis e que cada uma das ferramentas é capaz de oferecer funcionalidades distintas. Um desafio desse estudo é conseguir identificar as ferramentas que estão efetivamente alinhadas à necessidade da Agência. Por isso, a seguir será apresentado um quadro comparativo que avalia as funcionalidades levantadas a partir das necessidades da Agência para cada uma das ferramentas elencadas nos quadros acima.

		FABRICANTES							
		ELK	**Graylog**	**Paramount**	**Manage Engine**	**Netwrix**	**Varonis**	**StealthBITS**	**SailPoint**
FUNCIONALIDADES	**Active Directory**	**1.1**	**2.1**	**3.1**	**4.1**	**5.1**	**6.1**	**7.1**	**8.1**
	Auditoria de contas, computadores e grupos	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
	Auditoria de sites, GPO e outros recursos	Sim	Sim	-	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	-	-	-	-	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	-	-	-	Sim	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	-	-	-	Sim	Sim	Sim	Sim	Sim
	Automatiza tarefas repetitivas, comuns ou complexas	-	-	-	Sim	-	Sim	Sim	Sim
	Delegação de gerenciamento sobre grupos de segurança aos proprietários	-	-	-	-	-	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	-	-	-	Sim	Sim	Sim	-
	Servidores de Arquivos	**1.2**	**2.2**	**3.2**	**4.2**	**5.2**	**6.2**	**7.2**	**8.2**
	Auditoria de acesso, modificação e remoção de arquivos e pastas	Sim	Sim	-	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	Sim	Sim	-	-	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	-	-	-	-	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	-	-	-	Sim	Sim	Sim	Sim	Sim
	Automatiza tarefas repetitivas, comuns ou complexas	-	-	-	-	-	Sim	Sim	Sim
	Delegação de controle de acesso a proprietários	-	-	-	-	-	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	-	-	-	Sim	Sim	Sim	-
	Exchange	**1.3**	**2.3**	**3.3**	**4.3**	**5.3**	**6.3**	**7.3**	**8.3**
	Auditoria de acesso, modificação e remoção de caixas postais e listas.	Sim	Sim	-	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	-	-	-	Sim	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	-	-	-	-	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	-	-	-	Sim	Sim	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	-	-	-	Sim	Sim	Sim	-
	Descoberta e classificação de arquivos em repositórios não estruturados	**1.4**	**2.4**	**3.4**	**4.4**	**5.4**	**6.4**	**7.4**	**8.4**
	Identificação e classificação de conteúdos sensíveis	-	-	-	-	Sim	Sim	Sim	Sim
	% de atendimento dos requisitos	**29%**	**29%**	**5%**	**48%**	**52%**	**100%**	**100%**	**86%**

Pela tabela acima, é possível perceber que as ferramentas fornecidas pelas fabricantes Varonis e StealthBITS, dentre as que foram avaliadas neste estudo, possuem todas as necessidades levantadas no Documento de Oficialização de Demanda (Documento SEI 1572794) e possuem todas as necessidades detalhadas no item 3.2 deste estudo, que detalham os requisitos tecnológicos da solução.

É possível identificar que a ferramenta da SailPoint atende quase todas as funcionalidades definidas pelo requisitante, com exceção da funcionalidade de análise e monitoramento de comportamento dos usuários.

É possível identificar pela tabela acima, uma gama de ferramentas intermediárias, representadas pelos fabricantes *Manage Engine* e *Netwrix*. Essas ferramentas entregam funcionalidades de auditoria, porém se diferem quanto à possibilidade de execução de ações, envio de alertas e identificação e classificação de conteúdos sensíveis. Nenhuma dessas ferramentas possuem a funcionalidade de análise e monitoramento de comportamento de usuários.

Os números indicados na tabela acima identificam as ferramentas ou módulos que atendem as funcionalidades para cada produto (AD, servidores de arquivos, Exchange e descoberta e classificação de arquivos). A lista de ferramentas é detalhada na tabela abaixo.

Ferramentas	**Ferramenta 1**	**Ferramenta/Módulo 2**	**Ferramenta/Módulo 3**
1.1	Pilha ELK		
1.2	Pilha ELK		
1.3	Pilha ELK		
1.4	-		
2.1	Graylog		
2.2	Graylog		
2.3	Graylog		
2.4	-		
3.1	AD Security Audit Tool		
3.2	-		
3.3	-		
3.4	-		
4.1	AD Audit Plus	AD Manager Plus	
4.2	AD Audit Plus	AD Manager Plus	Exchange Reporter Plus
4.3	AD Audit Plus		
4.4	-		
5.1	Netwrix Auditor para AD		

5.2	Netwrix Auditor para servidores de arquivos		
5.3	Netwrix Auditor para Exchange		
5.4	Netwrix Auditor para servidores de arquivos		
6.1	Varonis DatAdvantage para Directory Services	Varonis DataPrivilege	Varonis DataAlert
6.2	Varonis DatAdvantage para Windows	Varonis DataPrivilege	Varonis DataAlert
6.3	Varonis DatAdvantage para Exchange	Varonis DataPrivilege	Varonis DataAlert
6.4	Varonis IDU Classification Framework		
7.1	StealthAUDIT for Active Directory	StealthAUDIT Action Modules	StealthINTERCEPT
7.2	StealthAUDIT for File Systems	StealthAUDIT Action Modules	StealthINTERCEPT
7.3	StealthAUDIT for Exchange	StealthAUDIT Action Modules	StealthINTERCEPT
7.4	StealthBits Sensitive Data Discovery and Classification		
8.1	SecurityIQ for Active Directory		
8.2	SecurityIQ for Windows shares and Unix file shares		
8.3	SecurityIQ for Exchange		
8.4	SecurityIQ for Windows shares and Unix file shares		

É possível perceber, pela tabela acima, que cada empresa possui um conjunto distinto de ferramentas e módulos, que agregados atendem à necessidade da Agência.

A *Varonis* possui 1 ferramenta, o *DatAdvantage,* que é aplicável aos serviços de diretório, de servidores de arquivos e de Exchange e que é ampliada com mais funcionalidades pela adição de módulos como o *DataPrivilege* e o *DataAlert*.

A *StealthBITS* possui 1 ferramenta, o *StealthAUDIT,* que é aplicável aos serviços de diretório, de servidores de arquivos e de Exchange e que é ampliada com mais funcionalidades pela adição de módulos como o *StealthAUDIT Action Module* e o *StealthINTERCEPT*.

Já a *SailPoint* possui somente uma ferramenta, o *SecurityIQ,* que é aplicável aos serviços de diretório, de servidores de arquivos e de Exchange.

Essa diversidade de ferramentas para cada fabricante, com a possibilidade ou não de adição de módulos, é um ponto essencial no agrupamento em lotes para a contratação.

5. ALTERNATIVAS/CENÁRIOS

Dentre as alternativas levantadas serão considerados para análise os seguintes cenários de contratação:

1. Soluções de software livre com contratação de suporte e licença empresarial.
2. Contratação de solução básica para auditoria de AD, Exchange e servidor de arquivos.
3. Contratação de solução intermediária para auditoria de AD, Exchange e servidor de arquivos.
4. Contratação de solução avançada para auditoria de AD, Exchange e servidor de arquivos, com licenciamento por subscrição/aluguel.
5. Contratação de solução avançada para auditoria de AD, Exchange e servidor de arquivos, com licenciamento perpétuo.

CENÁRIO 1	
Descrição	Soluções de software livre com contratação de suporte e licença empresarial.
Análise da Solução	É uma solução composta por ferramentas de gerenciamento de logs que permitiriam obter informações de auditoria do ambiente de AD, Exchange e servidores de arquivos pela recepção, tratamento e apresentação de informações. Dentre as alternativas apresentadas no tópico anterior deste estudo, identificam-se as ferramentas *ELK* e *Graylog*. **Pontos positivos:** • As ferramentas fornecidas por esses fabricantes permitiriam o gerenciamento dos logs de auditoria dos servidores e a possibilidade de criar alertas, painéis e executar ações no ambiente. • O custo de contratação de licença e suporte deste tipo de ferramenta é muito abaixo do custo de contratação de licenças para soluções especializadas. • As soluções são instaladas no ambiente de cliente e não são hospedadas na nuvem. • São soluções em software livre que poderiam ser utilizadas pela ANAC. Porém, há limite diária de armazenamento de dados para a solução gratuita da *Graylog* e estima-se que o limite não seria suficiente para atendimento da necessidade da Agência. **Pontos negativos:** • A ferramenta não fornece, nativamente, relatórios pré-definidos. • A criação de relatórios é possível, porém não há relatórios pré-definidos. • O envio de alertas é possível, porém não há alertas pré-definidos. • A execução de ações no ambiente é possível, porém a ferramenta não possui ações pré-definidas. • Não há funcionalidade de delegação de gerenciamento de acesso aos proprietários dos dados. • Não há funcionalidade de análise e classificação de conteúdos sensíveis. • Não há funcionalidade de análise de comportamentos suspeitos. • Alto custo financeiro de configuração de funcionalidades após a aquisição da licença, sem garantia de atendimento completo dos requisitos, devido à utilização de empresa terceirizada para configuração da ferramenta. Este tipo de solução não permitiria atender as necessidades após a contratação. Qualquer tipo de relatório, ação ou alerta necessitaria ser criado e aprimorado por equipe interna da ANAC. Funcionalidades solicitadas pelo requisitante como análise e classificação de arquivos, e monitoramento e bloqueio de comportamentos suspeitos de usuários, necessitariam de um esforço interno muito alto para serem implementadas, sem a garantia de que poderiam efetivamente ser implementadas. Considerando as informações apresentadas no documento SEI 2366433, uma estimativa diária de armazenamento no ambiente da ANAC de até 10 GB/dia e a cotação comercial do dólar no dia 25/10/2018 em R$ 3,70 por Dólar, a contratação da solução de gerenciamento de logs da *Graylog* teria um custo inicial aproximado de R$ 27.750,00 por ano. Este valor inclui o suporte à ferramenta e a licença anual do *Graylog Enterprise*. Conforme informações apresentadas em áudio-conferência realizada no dia 31/10/2018, com funcionário da empresa *Elastic,* fabricante da ferramenta ELK, a licença e suporte empresarial da ferramenta tem um custo aproximado de US$ 25.000,00 por

	instância, que licencia até 128 GB de memória. Um ambiente com alta disponibilidade necessitaria de ao menos 3 instância, e o custo aproximado seria de US$ 75.000,00. Considerando a cotação comercial do dólar do dia 30/10/2018, que foi de R$ 3.70 por dólar, o custo da licença empresarial e suporte da ferramenta ELK seria de aproximadamente R$ 277.000,00 por ano. Apesar do custo inicial estimado com a cotação enviada pela Graylog ser pequeno, o custo para fazer com que a ferramenta forneça as funcionalidades solicitadas pelo requisitante é muito alto. Além disso, o atendimento de todas as funcionalidades elencadas seria praticamente impossível e o tempo e esforço necessários para entrega das funcionalidades seria também alto. Com relação à ferramenta ELK, por ser uma ferramenta de gerenciamento e análise de logs de propósito geral, o custo da licença empresarial é mais cara. Porém, permitiria, além de obter muitas funcionalidades relacionadas à necessidade deste estudo, a possibilidade de análise de outros tipos de ambiente. Mesmo sendo uma ferramenta muito mais ampla que a *Graylog*, ela não atende todas as funcionalidades requisitadas pela área requisitante e ela necessitaria de um alto tempo e esforço para sua configuração. A solução fornecida pela *Paramount* não foi considerada nessa análise por apresentar grau muito baixo de atendimento das necessidades definidas pelo requisitante da solução. Por todos os motivos apresentados, **esse cenário não é recomendado para atendimento das necessidades da ANAC.**

CENÁRIO 2	
Descrição	Contratação de solução básica para auditoria de AD, Exchange e servidor de arquivos.
Análise da Solução	É uma solução composta por ferramentas desenvolvidas especificamente para auditoria do ambiente de AD, Exchange e servidores de arquivos. Dentre as alternativas apresentadas no tópico anterior deste estudo, identificam-se as fabricantes *Netwrix* e *Manage Engine.* **Pontos positivos:** • Atenderiam os requisitos relacionados a auditoria de AD, Exchange e servidores de arquivos. • Atenderiam os requisitos relacionados a geração de alertas. • A solução da Netwrix atenderia à necessidade de identificação e classificação de conteúdos sensíveis. • A solução da Netwrix atenderia à necessidade de análise e monitoramento de comportamento suspeitos de usuários. • A solução da *Manage Engine* atenderia à necessidade de execução de ações com objetos do AD e do Exchange. • Possui o menor custo benefício, considerando ferramentas específicas para auditoria de AD, Exchange e servidores de arquivos. **Pontos negativos:** • Apesar de monitorar o comportamento suspeito de usuários, a ferramenta da *Netwrix* não permite a execução de nenhum tipo de ação de bloqueio e tratamento com base nas informações auditadas. • As ferramentas não permitem a delegação de gerenciamento de acesso aos proprietários dos dados. • As ferramentas da *Manage Engine* não possuem funcionalidades para identificação e classificação de conteúdos sensíveis. As ferramentas analisadas neste cenário permitiriam atender parcialmente a necessidade da Agência, porém não atenderiam grande parte das necessidades. São ferramentas com o menor custo benefício dentre as soluções de auditoria específicas para *Active Directory*, *Exchange* e servidores de arquivos. Com base em proposta comercial da empresa AIQON Serviços em Informática Ltda (documento SEI 2366836), fornecedora no Brasil da fabricante *Netwrix*, a solução teria um custo anual de R$ 658.148,65, em caso de contratação de licença perpétua. Em caso de contratação de subscrição de licenças (Documento SEI 2366905), a proposta da empresa foi no valor de R$ 317.669,99. Neste caso específico, a aquisição de licença perpétua da solução se mostra mais vantajosa a partir de 3 anos do início do contrato. Para uma solução que a ANAC espera adquirir e utilizar no longo prazo, seria recomendada a aquisição das licenças. Além do uso no longo prazo, é importante destacar a impossibilidade de uso da solução em caso de término do contrato de subscrição e o prejuízo para a Agência pela impossibilidade de uso. Com base em proposta comercial da empresa ACSoftware (Documento SEI 2367093), fornecedora no Brasil da fabricante *Manage Engine,* a solução teria um custo de aquisição de licenças de R$ 251.428,30 por ano. Em caso de contratação de subscrição de licenças (Documento SEI 2367110), a solução teria um custo anual de R$ 109.916,40. Assim como no caso da empresa Netwrix e pelas mesmas justificativas, a aquisição de licença perpétua da solução se mostra mais vantajosa a partir de 3 anos do início do contrato. Destaca-se que empresas como Varonis, StealthBITS e Sailpoint também conseguiriam atender este cenário de contratação, porém as características mais avançadas das soluções fornecidas por elas fariam com que o custo fosse em torno de 3 vezes maior. Este cenário de contratação de licenças seria uma boa opção a ser considerada pela Agência em cenários de restrição de orçamento e com a readequação dos requisitos, pois conseguiria atender muitas funcionalidades com um bom custo benefício. Porém, ele não atende os requisitos detalhados no item 3 deste estudo. Ante o exposto, **o cenário não atende as necessidades elencadas pelo requisitante da solução.**

CENÁRIO 3	
Descrição	Contratação de solução intermediária para auditoria de AD, Exchange e servidor de arquivos
Análise da Solução	É uma solução composta por ferramentas desenvolvidas especificamente para auditoria do ambiente de AD, Exchange e servidores de arquivos. Dentre as alternativas apresentadas no tópico anterior deste estudo, identifica-se a fabricante *SailPoint.* **Pontos positivos:**

	• Atende os requisitos relacionados a auditoria de AD, Exchange e servidores de arquivos. • Atende os requisitos de execução de ações com objetos do AD, servidores de arquivos e do Exchange, inclusive para múltiplos objetos. • Atende os requisitos relacionados a geração de alertas com base nas informações auditadas. • Atende os requisitos para delegação de gerenciamento de acesso aos proprietários dos dados. • Atende os requisitos para identificação e classificação de conteúdos sensíveis. • Possui custo inferior às soluções apresentadas nos próximos tópicos. **Pontos negativos:** • Não possui funcionalidade de análise de comportamentos suspeitos de usuários. • Possui custo superior à soluções apresentadas nos cenários anteriores. As ferramentas analisadas neste cenário permitiriam atender praticamente toda a necessidade da Agência. Trata-se de solução com custo intermediário, mas que não atende a toda a necessidade levantada pelo requisitante. Com base em proposta comercial da empresa Netbr (documento SEI 2325935), fornecedora no Brasil da fabricante *Sailpoint*, a solução teria um custo anual de R$ 3.027.853,66, em caso de contratação de licença perpétua. A empresa não forneceu proposta de licenciamento por aluguel. Para uma solução que a ANAC espera adquirir e utilizar no longo prazo, seria recomendada a aquisição das licenças. Além do uso no longo prazo, é importante destacar a impossibilidade de uso da solução em caso de término do contrato de aluguel e o prejuízo para a Agência pela impossibilidade de uso. Destaca-se que empresas como Varonis e *StealthBITS* também conseguiriam atender este cenário de contratação, porém as características mais avançadas das soluções fornecidas por elas fariam com que o custo fosse aproximadamente 60% maior. As soluções de empresas como *Netwrix e Manage Engine* não conseguiriam atender esse cenário de contratação. Este cenário de contratação de licenças seria uma boa opção a ser considerada pela Agência caso os requisitos fossem readequados, pois conseguiria atender muitas funcionalidades com um custo menor. Porém, ele não atende os requisitos detalhados no item 3 deste estudo. Ante o exposto, **o cenário não atende as necessidades elencadas pelo requisitante da solução.**

CENÁRIO 4	
Descrição	Contratação de solução avançada para auditoria de AD, Exchange e servidor de arquivos, com licenciamento por subscrição/aluguel.
Análise da Solução	É uma solução composta por ferramentas de fabricantes como *Varonis* e *StealthBITS* cujo modelo de licenciamento é por subscrição ou aluguel. A solução considerada neste cenário permitiria atender toda a necessidade do requisitante. **Pontos positivos:** • As ferramentas fornecidas por esses fabricantes atendem as necessidades da Agência. • Modelo diferenciado de cobrança de aluguel de uso da licença, podendo implicar em redução de custos ou diluição do custo de uma solução mais cara de acordo com a quantidade de usuários auditados. • As soluções são instaladas no ambiente de cliente e não são hospedadas na nuvem. • Não há diferenças em relação às funcionalidades das ferramentas nesse modelo de licenciamento ou no modelo de licenciamento por aquisição. **Pontos negativos:** • Apresenta fragilidades no quesito de continuidade do negócio, já que o encerramento do contrato pode sujeitar a agência à suspensão imediata dos serviços e a perda ao direito de uso ou acesso às informações auditadas e armazenadas. • Dentre as contratações da Administração Pública Federal (APF) levantadas no tópico anterior desse estudo, somente o Pregão MPT/PGT 39, de 2017, optou por esse modelo. Porém, a necessidade atendida nesse pregão não é comparável à necessidade da ANAC. • Houve dificuldade na comparação de custos, pois as empresas não forneceram propostas para esse modelo de licenciamento. • Não há diminuição na necessidade de equipe técnica operacional necessária para manutenção da infraestrutura da solução. • Após o término do contrato, a solução é bloqueada e não é mais possível ter acesso às informações auditadas. Com base nos pontos negativos apresentados, este cenário é bastante arriscado e poderia causar problemas futuros para a Agência em relação à necessidade contínua de auditorias. Apesar de atender todos os requisitos, **este não é um cenário recomendado para contratação** devido ao ponto negativo relacionado a continuidade do serviço após o término do contrato. Apesar de não ter sido possível a comparação com os custos de aquisição das licenças, é provável, considerando o exposto no cenário 2, que a aquisição de licenças demonstre ser mais vantajosa a partir do terceiro ano de contrato.

CENÁRIO 5	
Descrição	Contratação de solução avançada para auditoria de AD, Exchange e servidor de arquivos, com licenciamento perpétuo.
Análise da Solução	É uma solução composta por ferramentas de fabricantes como Varonis e SteathBITS, cujo modelo de licenciamento é perpétuo. A solução considerada neste cenário permitiria atender toda a necessidade do requisitante. **Pontos positivos:** • As ferramentas fornecidas por esses fabricantes atendem as necessidades da Agência. • As soluções são instaladas no ambiente de cliente e não são hospedadas na nuvem.

	• Não há diferenças em relação às funcionalidades das ferramentas nesse modelo de licenciamento ou no modelo de licenciamento por subscrição. • Após o término do contrato, a ferramenta poderá ser utilizada normalmente. • Dentre as contratações da Administração Pública Federal (APF) levantadas no tópico anterior desse estudo, a grande maioria opta por esse modelo. • É um modelo de licenciamento que garante a continuidade do negócio após o termino do contrato. **Pontos negativos:** • Após o término do contrato de suporte, a solução fica operacional mas não há o fornecimento de novas versões dos produtos. • A Agência paga pelo quantitativo atual de usuários ativos da rede e, caso necessite aumentar o quantitativo, será necessária alteração contratual ou nova contratação. • Após o término do contrato, pode ser necessário novo contrato de suporte para acesso às versões mais atualizadas da solução. • O custo aproximado dos contratos de suporte são em torno de 20% do valor total dos produtos por ano de contrato. Este é o único cenário que atende os requisitos da solução identificado no item 3 deste estudo, e, por isso, **este é o cenário recomendado para contratação.**

5.1. **Observância das alternativas às políticas, premissas e especificações técnicas vigentes**

Requisito	ID do cenário	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	X		
	2	X		
	3		X	
	4		X	
	5	X		
A Solução está disponível no Portal do Software Público Brasileiro?	1		X	
	2		X	
	3		X	
	4		X	
	5		X	
A Solução é um software livre ou software público?	1		X	
	2		X	
	3		X	
	4		X	
	5		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1	X		
	2	X		
	3	X		
	4	X		
	5	X		
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			X
	2			X
	3			X
	4			X
	5			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	1			X
	2			X
	3			X
	4			X
	5			X

5.2. **Orçamento estimado**

A presente contratação está descrita no PDTI 2018/2019 conforme apresentado abaixo:

- **Lote:** Solução para gestão, monitoração, auditoria, automação e prevenção de perdas de dados no AD
- **Natureza da Despesa:** Aquisição de Software
- **Código da Despesa:** 44903993
- **Valor estimado - 2018:** R$ 60.000,00
- **Valor estimado - 2019:** R$ 60.000,00
- **Serviço continuado:** Sim
- **Projetos PDTI para os quais contribuirá:** PR18CP0048

6. ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DE PROPRIEDADE DAS SOLUÇÕES IDENTIFICADAS

Os cenários 1, 2 e 3 apresentados no tópico anterior não atendem as necessidades descritas pela área requisitante e que foram detalhadas no documento SEI 1572794 (DOD - Documento de oficialização da demanda) e no tópico 3 deste estudo. Estes cenários apresentam soluções que permitiriam atender apenas parte dos requisitos e, por isso, não são considerados com cenários que atendem a necessidade da Agência. Os custos identificados para esses cenários variam desde R$ 27.000,00, no cenário 1, até R$ 3.000.000,00, no cenário 3. As soluções avaliadas no cenário 2 possuem custo estimado entre R$ 250.000,00 e 660.000,00.

É possível perceber, através de uma tabela comparativa entre fabricantes e funcionalidades apresentada no tópico 4.4.2 deste estudo,

que a diferença entre a solução analisada no cenário 3 e as soluções analisadas nos cenários 4 e 5 está associada à funcionalidade de monitoramento e análise de comportamentos suspeitos de usuários para os serviços de AD, Exchange e servidores de arquivos. Isto é, a solução identificada no cenário 3 não teria esta funcionalidade, enquanto que as soluções identificadas nos cenários 4 e 5 teriam as funcionalidades.

Segundo demostrado pela área requisitante da solução no DOD - Documento de oficialização da demanda -, a funcionalidade de monitoramento e análise de comportamento suspeito de usuários é justificável pelos seguintes fatores:

- Impossibilidade, com base no uso das ferramentas atuais utilizadas na ANAC, de identificar acessos indevidos de usuários internos mal-intencionados ou incidentes de segurança cibernética de forma rápida e precisa.
- Auxiliar no atendimento das diretrizes de Segurança da Informação de Comunicações instituída pela Norma Complementar nº 20/IN01/DSIC/GSIPR, de dezembro de 2014, especificamente em relação ao item 4.10 e outros itens correlatos existentes na norma.
- Implementar padrões de Gestão de Segurança da Informação recomendados na norma ABNT NBR ISO/IEC 27002:2013 - Código de Prática para a Gestão da Segurança da Informação - , especificamente em relação aos itens 10.10.1 e 10.10.2.

> "10.10.1 - Registros de auditoria
>
> Controle: Convém que **registro** (log) de auditoria contendo atividades dos usuários, exceções e outros **eventos de segurança da informação** sejam produzidos e mantidos por um período de tempo acordado **para auxiliar em futuras investigações e monitoramento de controle de acesso**.
>
> ...
>
> 10.10.2 - Monitoramento do uso do sistema:
>
> Controle: Convém que sejam estabelecidos procedimentos para o **monitoramento do uso** dos recursos de processamento da informação e os resultados das **atividades de monitoramento sejam analisados criticamente**, de forma regular.

- adequação contínua das capacidades de controle e monitoramento necessárias aos serviços alocados no ambiente da ANAC, aumentando o gerenciamento, eficiência e proteção das informações, simplificando tarefas complexas e permitindo uma fácil adaptação dos analistas e administradores da TI a alterações de emergência ou imprevistas.

Em relação ao Cenário 4 apresentado no tópico anterior, não foi possível identificar contratações na Administração Pública que estivessem alinhadas à necessidade da Agência e que optassem por aluguel das licenças. Além disso, apesar de terem sido enviadas solicitações de cotação para o modelo de aluguel de licenças, as fornecedoras das empresas *Varonis* e *StealthBITS* não enviaram cotações. Por isso, não foi possível avaliar o custo total de propriedade para o cenário 4.

Dentre as alternativas levantadas neste estudo, o cenário 5 é o único que demonstrou estar aderente às necessidades da Agência.

Durante as fases iniciais de elaboração deste estudo técnico, imaginava-se que a contratação seria atendida com um serviço de suporte e garantia de 12 meses. Nesse contexto, as primeiras cotações recebidas que são consideradas no cenário 5, apresentadas nos documentos SEI 2325482, 2325552 e 2325647, consideraram a aquisição da solução com serviços de suporte e garantia por um período de 12 meses. Para essa primeira pesquisa, realizada em setembro de 2018, o custo da contratação estimado ficou em R$4.791.930,00.

Com o andamento do processo de contratação e definição de que o período de suporte e garantia adequado para a solução deveria ser de 36 meses, foi necessária a solicitação de nova cotação de preços, executada apenas em março de 2019. Este prazo de garantia e suporte técnico é necessário para garantir que a solução continuará atualizada à medida que forem surgindo novas versões dos softwares auditados e, além disso, para garantir seu completo funcionamento durante um período de vida útil mínimo para o produto. Aliado a isso, verifica-se ainda que diversas outras contratações relacionadas a esse tipo de solução tem por padrão a contratação dos serviços de suporte e garantia pelo prazo solicitado.

Serão considerados na comparação de custos as seguintes opções:

1. Pregão eletrônico 38/2018 da ANTT (Documento SEI 2833887)
2. Pregão eletrônico 04/2017 do MEC/INEP. (Documento SEI 2325988)
3. Pregão 03/2017 do CONFEA. (Documento SEI 2326003)
4. Cotação enviada pela empresa INFOSEC Tecnologia da informação Ltda., fornecedora de soluções da fabricante *Varonis*. (Documento SEI 2833022)
5. Cotação enviada pela empresa Omega Tecnologia da Informação Ltda., fornecedora de soluções da fabricante *Varonis*. (Documento SEI 2833042)
6. Cotação enviada pela empresa ISH Tecnologia S/A, fornecedora de soluções da fabricante *StealthBITS*. (Documento SEI 2833077)

Item do objeto da contratação	Descrição dos produtos	Qtd.	Proposta com menor preço	Preço MÉDIO	
				Média do valor unitário das propostas (R$)	Média do valor Total das propostas (R$)
1	Solução de auditoria para Active Directory - 2.400 usuários ativos - Análise de comportamento suspeito - Delegação de gerenciamento de permissões - Execução de ações proativas	2400	Pregão do CONFEA 03_2017	R$419,40	R$1.006.562,00
2	Solução de auditoria para servidores de arquivos - 2.400 usuários ativos - Análise de comportamento suspeito - Delegação de gerenciamento de permissões - Execução de ações proativas	2400	Pregão do CONFEA 03_2017	R$515,49	R$1.237.172,00
3	Solução de auditoria para Exchange - 2.400 usuários ativos - Análise de comportamento suspeito - Execução de ações proativas	2400	Pregão do CONFEA 03_2017	R$515,49	R$1.237.172,00
4	Solução para classificação de arquivos - Identificação e classificação de conteúdos sensíveis	2400	Pregão do CONFEA 03_2017	R$424,98	R$1.019.958,00

5	Serviços de suporte técnico e garantia - Mensal - 2.400 usuários ativos	36	Proposta da Empresa Infosec	R$82.041,80	R$2.953.504,80
6	Treinamento para as ferramentas contratadas - 1 turma - Até 8 alunos	1	Pregão do CONFEA 03_2017	R$51.183,00	R$51.183,00
				Total	**R$7.505.551,80**

O cálculo do valor médio da contratação apresentado no quadro acima não considerou os valores dos pregões 04/2017 do MEC/INEP e 38/2018 da ANTT por possuirem valores por item bem superiores aos preços do Pregão 03/2017 do CONFEA e aos preços obtidos nas cotações enviadas pelas empresas. O que é possível perceber ao se comparar as diversas contratações é que, quando a contratante não especifica um item para os serviços de suporte e garantia, como é o caso dos pregões do MEC e da ANTT, a empresa contratada agrega o valor do serviço ao preço individual de cada item de solução contratado.

Ao se calcular o valor médio da contratação apenas considerando os pregões do MEC e da ANTT, que não especificam um item para os serviços de suporte técnico e garantia, percebe-se que a média é 3,2% superior ao apresentado na tabela acima.

Vale notar que a estimativa de preços baseada na comparação com contratações similares torna-se bastante complexa e relativamente imprecisa, em razão da diversidade e peculiaridade próprias de cada ambiente de Tecnologia de Informação, como, por exemplo, quantidade de licenças a serem adquiridas, treinamentos, serviços de garantia para os itens contratados, entre outras peculiaridades.

Nas contratações realizadas por outros órgãos da Administração Pública, os órgãos optaram pela especificação de itens distintos que forneceriam as funcionalidades de análise de comportamento suspeito e de delegação de gerenciamento de permissões. No entanto, o estudo demonstrou que essas funcionalidades podem também ser agregadas em uma única solução, como é o caso da solução da *SailPoint*, ou em módulos distintos, como é o caso da solução da *StealthBITS*. Assim, para efeito de comparação e para aumentar a concorrência entre fornecedores, é preferível a definição de itens relacionados a soluções para *Active Directory*, servidores de arquivos ou *Exchange* que agreguem todas as funcionalidades especificadas pelo requisitante para cada serviço. Por isso, para fornecer a solução relacionada a *Active Directory*, uma empresa poderá fornecer apenas um sistema que possua todas as funcionalidades ou agregar vários sistemas em uma única interface para fornecer todas as funcionalidades. A mesma situação ocorrerá também para as soluções de auditoria de servidores de arquivos e de Exchange, itens 2 e 3 da tabela.

Por outro lado, todas as fabricantes possuem soluções específicas que fornecem a funcionalidade de identificação e classificação de conteúdos sensíveis e, assim, optou-se por especificar esse item de forma separada.

Diante de todas essas particularidades entre o analisado neste estudo e as contratações realizadas por outros órgãos da administração, para a comparação de custos foi necessário agrupar itens que em outros contratações eram itens separados e também readequar os quantitativos de licenças contratadas com base na quantidade de licenças necessárias na ANAC.

O custo total estimado para essa contratação é de R$ 7.505.551,80, demonstrando ser bastante superior ao previsto no PDTI 2018/2019, exposto no tópico 5.2 deste estudo, que previa um custo de R$ 60.000,00. Por isso, para prosseguir com a contratação, seria necessária a realocação de recursos orçamentários por parte da Agência.

Apesar de não ser possível comparar os valores do cenário 5 (aquisição) com o cenário 4 (aluguel), pela impossibilidade de se obter propostas de fabricantes ou por não haver contratações da Administração Pública compatíveis com a necessidade da ANAC para o cenário 4, é importante destacar que o Cenário 4 gera dependência da Agência com relação ao fabricante da solução, pois a ANAC poderia perder o acesso aos dados de auditoria em caso de término do contrato de aluguel de licenças. Considerando que a auditoria de dados históricos atende a princípios da Política de Governança de Informações Digitais da ANAC, atende a padrões da norma ISO/IEC 27002:2013 e que a solução contratada pretende corrigir o processo de gestão de infraestrutura de TI a falhas encontradas pela Auditoria interna da ANAC, a contratação pelo Cenário 4 seria muito arriscada e não recomendada..

7. ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

7.1. Análise

Os seguintes pontos foram considerados para a escolha da solução:

- Pontos positivos e negativos dos cenários apresentados no tópico 5 deste estudo;
- Aderência às necessidades elencadas pela área requisitante;
- Opções disponíveis na Administração Pública e no mercado;
- Recomendações do Ministério do Planejamento, Desenvolvimento e Gestão em relação à aquisição de soluções de Tecnologia da Informação;
- Impacto para a continuidade do serviço após o término do contrato;
- Aderência aos normativos de auditoria de TI;
- Achados da Auditoria Interna de falhas no processo de gestão de identidade;
- Alinhamento a padrões e práticas de mercado relacionados a Gestão de Segurança da Informação;

Tomando por base todos esses pontos, o cenário que demonstrou ser tecnicamente viável é o de contratação de solução de mercado com licenciamento perpétuo, apresentado no cenário 5 deste estudo.

7.2. Descrição da solução de Tecnologia da Informação

Aquisição de licenças perpétuas para solução de auditoria, gestão, automação e delegação do gerenciamento de serviços do AD (*Microsoft Active Directory*), correio eletrônico (*Microsoft Exchange Server*) e servidores de arquivos (*Microsoft File Server*). A solução deve monitorar os usuários em tempo real, identificar desvios de comportamento, permitir delegação de gerenciamento de acesso aos proprietários dos dados, executar ações proativas em múltiplos objetos, e identificar e classificar conteúdos sensíveis. A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução.

ID	Bem/Serviço	Estimativa*
1	Solução de auditoria e outras funcionalidades para Microsoft *Active Directory,* 2.400 usuários e com licença perpétua.	R$ 1.006.562,00
2	Solução de auditoria e outras funcionalidades para servidores de arquivos, 2.400 usuários e com licença perpétua.	R$ 1.237.172,00
3	Solução de auditoria e outras funcionalidades para *Microsoft Exchange,* 2.400 usuários e com licença perpétua.	R$ 1.237.172,00
4	Solução para identificação e classificação de conteúdos sensíveis, 2.400 usuários e com licença perpétua	R$ 1.019.958,00
5	Serviços de suporte técnico e garantia para todas as soluções, por 36 meses	R$ 2.953.504,80
10	Treinamento para as soluções contratadas - 10 participantes	R$ 51.183,00
Total =		**R$ 7.505.551,80**
* A estimativa foi feita com base na análise de outras contratações da Administração Pública e em propostas de fornecedores, adaptados de acordo com os itens e quantitativos necessários.		

7.3. **Alinhamento em relação às necessidades de negócio e aos macro requisitos tecnológicos**

Alinhamento ao Planejamento Estratégico Institucional – PEI - 2015/2019

- Objetivo estratégico "2.3 Garantir a Efetividade da Prestação de Serviços de TI" - “Perspectiva dos Processos Internos”
  - “Estratégia 2.3.1 - Aprimorar o atendimento de demandas dos usuários da TI”
    - “Iniciativa 2.3.1.3 - Otimizar o processo de atendimento a usuários de TI”
    - “Iniciativa 2.3.1.4 - Otimizar o modelo de governança de TI”

Alinhamento Planejamento Estratégico de Tecnologia da Informação - PETI - 2016/2019

– “Objetivo 6: Aprimorar o atendimento de demandas dos usuários de TI" - "Perspectiva: Processos Internos"

“Iniciativa 6.3. Otimizar o processo de atendimento a usuários de TI”;

A solução está descrita no PDTI 2018-2019 com o código PR18CP0048.

A solução escolhida está alinhada às necessidades e requisitos tecnológicos descritos no tópico 3 deste estudo.

7.4. **Identificação dos benefícios a serem alcançados com a solução**

- Garantir níveis satisfatórios de segurança da informação no âmbito da TI;
- Garantir a efetividade da prestação de serviços de TI;
- Criar e implementar plano de adequação de infraestrutura de TI;
- Aprimorar a gestão da informação para a tomada de decisão;
- Implantar um sistema de segurança da informação e comunicações;
- Instituir o modelo de governança corporativa da ANAC;
- Estruturar o processo de gestão corporativa de riscos;
- Instituir sistema de gestão corporativa de riscos;
- Aumentar o nível de atendimento e qualidade das operações de serviços de TI;
- Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente de arquivos;
- Automação de controle de privilégios aos curadores dos dados e informações;
- Classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos;
- Análise comportamental dos usuários internos no ambiente computacional reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados;
- Aprimorar a governança de TI;
- Aprimorar governança de dados, informação e conhecimento;
- Aprimorar a gestão de segurança da informação e comunicações;
- Disponibilização de segurança e auditoria ininterrupta dos serviços de correio eletrônico, compartilhamento de arquivos e serviços de diretórios.

8. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA VIABILIZAR A EXECUÇÃO CONTRATUAL

Não foi possível identificar necessidades de adequação tecnológica, elétrica, logística, de espaço físico, mobiliário ou qualquer outra necessidade de ambiente.

9. AVALIAÇÃO E DEFINIÇÃO DOS RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

9.1. **Recursos Materiais**

RECURSO	DISPONIBILIDADE	AÇÃO	RESPONSÁVEL
Ambiente de virtualização para hospedar as máquinas virtuais onde será instalada a solução	Integral	Verificar e validar junto à área de TI que ficará responsável pela fiscalização técnica do contrato.	ANAC
Espaço de armazenamento para retenção das informações auditadas.	Integral	Solicitar e verificar junto à área responsável pela administração da solução de armazenamento.	ANAC

Banco de dados para armazenamento de informações	Integral	Providenciar junto à área responsável pela administração da solução de banco de dados	ANAC
Manuais técnicos do usuário e de referência, contendo todas as informações sobre os produtos, com instruções para instalação, configuração, operação e administração da solução	Integral	Documentação exigida na contratação da solução	Empresa vencedora do certame para fornecimento da solução

9.2. **Recursos Humanos**

Durante a execução do Contrato a ser firmado, os recursos humanos e processos organizacionais necessários à implementação de seu objeto referem-se à configuração, instalação e monitoração da solução, à fiscalização e à gestão do contrato.

Em relação aos recursos humanos, verifica-se a necessidade de se manter o quantitativo de pessoal adequado à composição da Equipe de Fiscalização e Gestão do Contrato a ser firmado, conforme apresentado abaixo.

RECURSO	FORMAÇÃO	ATRIBUIÇÃO	PRAZOS E PERIODICIDADE	RESPONSÁVEL PELA OBTENÇÃO DO RECURSO
Preposto	Funcionário da contratada	Interlocutor da empresa vencedora do certame, que tratará de questões cotidianas e administrativas referentes ao contrato.	De acordo com disponibilidade especificada nos requisitos e durante a vigência do contrato e da garantia da solução	Empresa contratada
Fiscal Técnico do Contrato	Servidor da Agência	Acompanhar implantação da solução, atestar o funcionamento de cada módulo contratado, e, no caso de falhas ou dúvidas, acionar o suporte técnico especializado contratado junto com a solução para garantir manutenção, operacionalidade e atualizações	Cotidiano	ANAC
Fiscal Administrativo do Contrato	Servidor da Agência.	Fiscalizar o contrato, do ponto de vista administrativo da Solução de TIC	Cotidiano	ANAC
Fiscal Requisitante do Contrato	Servidor da Agência.	Fiscalizar o contrato, do ponto de vista funcional da Solução de TIC.	Cotidiano	ANAC
Gestor do Contrato	Servidor da Agência.	Acompanhamento das questões administrativas do contrato	Cotidiano	ANAC

10. **ESTRATÉGIA DE CONTINUIDADE CONTRATUAL**

Evento 1	
Não entregar os objetos contratados	
Ação Preventiva	Verificar as condições de habilitação da empresa contratada
Responsáveis	Gerência de licitações e contratos
Ação de contingência	Chamar 2ª colocada no certame, e assim sucessivamente, ou o objeto terá que ser novamente licitado
Responsáveis	Gerência de licitações e contratos
Evento 2	
Atraso na entrega dos produtos	
Ação Preventiva	Solicitar cronograma de entregas e realização da reunião inicial nos dias seguintes à assinatura do contrato.
Responsáveis	Equipe de fiscalização do contrato
Ação de contingência	Acionar o fornecedor para definir a data de entrega e tomar medidas administrativas previstas em contrato, informar o gestor do contrato sobre o atraso e sanções cabíveis em contrato, verificar com a área requisitante o impacto na área de negócio.
Responsáveis	Fiscal Técnico e Fiscal Administrativo
Evento 3	
Encerramento abrupto do contrato	
Ação Preventiva	Verificar a capacidade da empresa para a entrega dos produtos no prazo, verificar a capacidade da empresa para atender a garantia solicitada em contrato, acompanhar a resposta dos chamados.
Responsáveis	Fiscal Técnico e Fiscal Administrativo
Ação de contingência	Tomar as ações administrativas cabíveis em contrato e na legislação, informar o gestor do contrato das sanções administrativas previstas no contrato, informar o fornecedor sobre as sanções a serem realizadas
Responsáveis	Fiscal Administrativo e Gestor do contrato
Evento 4	
Vencimento de prazo de garantia e de suporte técnico da solução	
Ação Preventiva	Observar os prazos de garantia e suporte técnico da solução para garantir tempo hábil para a elaboração de nova contratação
Responsáveis	Equipe de fiscalização do contrato
Ação de contingência	Incluir nova contratação no planejamento de contratações de TI
Responsáveis	Superintendência de Tecnologia

11. **DECLARAÇÃO DE VIABILIDADE**

Em atendimento ao disposto na Instrução Normativa MP/SLTI nº 04/2014, art. 12, inciso VIII, realiza-se agora a declaração de viabilidade da contratação.

O presente Estudo Técnico Preliminar (ETP) foi elaborado de acordo com o previsto na Instrução Normativa MP/SLTI nº 04/2014, art. 12. Conforme esse dispositivo, foram levantados os requisitos da solução, avaliadas as soluções identificadas, escolhida e justificada a solução a ser contratada.

Diante do exposto, a Equipe de Planejamento da Contratação declara que **a solução escolhida por meio deste estudo é tecnicamente viável**, contudo, o PDTI 2018-2019, de fevereiro de 2018, possui previsão orçamentária para o projeto PR18CP0048 de apenas R$ 60.000,00. **Sendo assim, sua viabilidade econômica depende da realocação de recursos por parte da Agência.**

12. ASSINATURAS

Integrante Técnico	
Nome: MARCELO AUGUSTO CURADO FLEURY TEIXEIRA	Matrícula/SIAPE: 2030374
O presente planejamento foi elaborado em harmonia com a Instrução Normativa nº 4/2014 – Secretaria de Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis com a realidade de mercado, porém incompatíveis com a previsão do PDTI 2018/2019, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos. Assim, recomendamos a aquisição proposta desde que sejam realocados recursos para a contratação.	

Integrante Requisitante	
Nome: MARCELO NOGUEIRA LINO	Matrícula/SIAPE: 2126657
O presente planejamento está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.	

Autoridade Competente	
Nome: GUSTAVO SANCHES	Matrícula/SIAPE: 2295079
O presente planejamento está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão, mesmo que os integrantes técnico e/ou requisitante tenham se pronunciado pela inviabilidade da contratação. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área responsável priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.	

Documento assinado eletronicamente por **Marcelo Augusto Curado Fleury Teixeira**, **Analista Administrativo**, em 02/04/2019, às 18:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcelo Nogueira Lino**, **Gerente**, em 26/06/2019, às 12:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Gustavo Sanches**, **Superintendente de Tecnologia da Informação**, em 26/06/2019, às 17:58, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sistemas.anac.gov.br/sei/autenticidade, informando o código verificador **1897709** e o código CRC **93A057DF**.