SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

SEPN 508, Bloco A Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho - Bairro Asa Norte, Brasília/DF, CEP 70740-541

Contato: - http://www.confea.org.br

EDITAL DE LICITAÇÃO Nº 90003/2026

Processo: 00.003608/2024-71

PREGÃO ELETRÔNICO Nº 90003/2026
CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA
Processo Administrativo n° 00.003608/2024-71

Torna-se público, para conhecimento dos interessados, que o(a) Conselho Federal de Engenharia e Agronomia - CONFEA, CNPJ nº 33.665.647/0001-91, por meio do(a) Comissão de Contratação instituída pela Portaria nº 364/2024, sediado(a) SEPN 508, Bloco A, Edifício Confea - Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, na cidade de Brasília/DF, CEP: 70740-541, realizará licitação, para registro de preços, na modalidade Pregão Eletrônico, na forma Eletrônica, com critério de julgamento Menor Preço por Lote, Lei nº 14.133, de 1º de abril de 2021, do Decreto nº 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital e seus anexos.

Data da Sessão Pública: 17/04/2026

Hora Inicial 8:30

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de solução de tecnologia da informação e comunicação para gerenciamento de exposição, compreendendo licenciamento de software, serviços especializados, suporte técnico, treinamento e serviços continuados, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formado por 7 (sete) itens, conforme tabela constante no Termo de Referência do anexo I deste edital, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços no anexo III deste Edital.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste certame os interessados cujo ramo de atividade seja

compatível com o objeto da licitação e que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

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

3.3. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

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

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

3.6. Para os itens não será concedido tratamento favorecido para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Leis nº 8.248, de 23 de outubro de 1991 e art. 8º do Decreto nº 7.174, de 2010.

3.7. Não poderão disputar esta licitação:

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

3.7.2. sociedade que desempenhe atividade incompatível com o objeto da licitação;

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

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

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

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

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

3.7.8. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1986, concorrendo entre si;

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

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

3.8. sociedades cooperativas;

3.8.1. pessoas jurídicas reunidas em consórcio;

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

3.10. O impedimento de que trata o item 3.7.6 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.11. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.7.4 e 3.7.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

3.13. O disposto nos itens 3.7.4 e 3.7.5 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

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

3.15. A vedação de que trata o item 3.9 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. ORÇAMENTO ESTIMADO SIGILOSO

4.1. O orçamento estimado da presente contratação não será de caráter sigiloso.

4.2. O custo estimado total da contratação é de R$ 48.349.223,32 (quarenta e oito milhões, trezentos e quarenta e nove mil duzentos e vinte e três reais e trinta e dois centavos).

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

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

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

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

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

5.3.2. não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (quatorze)

anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

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

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

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

5.5. A falsidade da declaração de que trata no item 5.4 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

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

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

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

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

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

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

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

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

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

5.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 5.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

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

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

6. DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema

eletrônico, dos seguintes campos:

6.1.1. Valor expresso em Reais (R$).

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

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

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 execução do objeto.

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

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.

6.5.1. No regime de incidência não-cumulativa de PIS e COFINS, a cotação adequada será a que corresponde à média das alíquotas efetivamente recolhidas pela empresa, comprovada, a qualquer tempo, por documentos de Escrituração Fiscal Digital da Contribuição (EFD-Contribuições) para o PIS/PASEP e COFINS dos últimos 12 (doze) meses anteriores à apresentação da proposta, ou por outro meio hábil.

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

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

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

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;

6.11. Os licitantes devem respeitar os preços máximos previstos no Termo de Referência/Projeto Básico;

6.12. O descumprimento das regras supramencionadas 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 automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

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

pública.

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

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

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

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 ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,01% (zero vírgula zero um por cento) .

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

7.10. O procedimento seguirá de acordo com o modo de disputa aberto.

7.11. No modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

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

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

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

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

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

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

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

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

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

7.18. Será assegurado o direito de preferência previsto no artigo 3º da Leis nº 8.248, de 23 de outubro de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

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

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

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

7.18.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Leis nº 8.248, de 23 de outubro de 1991.

7.18.2. Os licitantes classificados que estejam enquadrados no item 7.18.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

7.18.3. Caso a preferência não seja exercida na forma do item 7.18.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 7.18.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 7.18.1.3 caso esse direito não seja exercido.

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

7.19. Só poderá haver empate entre propostas iguais (não seguidas de lances).

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

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

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

7.20.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, nos termos do Decreto nº 11.430, de 2023, e da Instrução Normativa SEGES/MGI nº 382, de 17 de setembro de 2025;

7.20.4. desenvolvimento pelo licitante de programa de integridade, conforme Decreto n° 12.304, de 2024, e Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025 .

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

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

7.21.2. empresas brasileiras;

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

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

7.22. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão

convocados, vedado qualquer outro processo.

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

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

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

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

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

7.23.5. O Pregoeiro solicitará ao licitante mais bem classificado que, no prazo d e 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.

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

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

8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o Pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no item 3.8 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.1.1. SICAF;

8.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;

8.1.3. Cadastro Nacional de Empresas Punidas – CNEP e

8.1.4. Lista de licitantes inidôneos, mantida pelo Tribunal de Contas da União.

8.2. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

8.2.1. A consulta no CEIS quanto às sanções previstas na Lei n° 8.429, de 1992, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

8.3. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas ao CEIS, CNEP e Lista de licitantes inidôneos pela Consulta Consolidada de Pessoa Jurídica do TCU.

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

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

8.4.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

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

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

8.6. Será desclassificada a proposta vencedora que:

8.6.1. contiver vícios insanáveis;

8.6.2. não obedecer às especificações técnicas contidas no Termo de Referência/Projeto Básico;

8.6.3. apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação;

8.6.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

8.6.5. não cumpra os critérios de aceitabilidade de preços definidos no Termo de Referência.

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

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

8.8. A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência do Pregoeiro, que comprove:

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

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

8.9. Em contratação de obras e serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

8.9.1. Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, contratação semiintegrada ou contratação integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

8.9.2. No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado.

8.9.3. No caso de obras e serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

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

8.11. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

8.11.1. Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e

dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semiintegrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

8.11.2. Caso a produtividade seja diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

8.11.3. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

8.11.4. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

8.12. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;
8.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;
8.12.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.13. 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.

8.14. Caso o Termo de Referência exija a apresentação de carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor, o licitante classificado em primeiro lugar deverá apresentá-la, sob pena de não aceitação da proposta.

8.15. Caso o Termo de Referência/Projeto Básico exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.16. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.17. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.18. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.19. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

9. DA FASE DE HABILITAÇÃO

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

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

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

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

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

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

9.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei .

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

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

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

9.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

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

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

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

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

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

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

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

9.13. Encerrado o prazo para envio da documentação de que trata o item 9.11.1, poderá ser admitida, mediante decisão fundamentada do Pregoeiro, a apresentação de novos documentos de habilitação ou a complementação de informações acerca dos documentos já apresentados pelos licitantes, em até 2 (duas) horas, para:

9.13.1. a aferição das condições de habilitação do licitante, desde que decorrentes de fatos existentes à época da abertura do certame;

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

9.13.3. suprimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante;

9.13.4. suprimento da ausência de certidão e/ou documento de cunho declaratório expedido por órgão ou entidade cujos atos gozem de presunção de veracidade e fé pública.

9.14. Findo o prazo assinalado sem o envio da nova documentação, restará preclusa essa oportunidade conferida ao licitante, implicando sua inabilitação.

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

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

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

10. DO TERMO DE CONTRATO

10.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado termo de contrato, ou outro instrumento equivalente.

10.2. O adjudicatário terá o prazo de 2 (dois) dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato ou instrumento equivalente, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

10.3. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá:

10.3.1. encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), para que seja assinado e devolvido no prazo de 2 (dois) dias úteis, a contar da data de seu recebimento;

10.3.2. disponibilizar acesso a sistema de processo eletrônico para que seja assinado digitalmente em até 2 (dois) dias úteis; ou

10.3.3. outro meio eletrônico, assegurado o prazo de 2 (dois) dias úteis para resposta após recebimento da notificação pela Administração.

10.4. Os prazos dos itens 10.2 e 10.3 poderão ser prorrogados, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

10.5. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

10.6. Na assinatura do contrato ou instrumento equivalente será exigido o Cadastro Informativo de Créditos não Quitados do Setor Público Federal - Cadin e a comprovação das condições de habilitação e contratação consignadas neste Edital, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

10.6.1. A existência do registro do Cadin constitui fator impeditivo para a contratação.

11. DA ATA DE REGISTRO DE PREÇOS

11.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 2 (dois) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

11.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

11.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e

11.2.2. a justificativa apresentada seja aceita pela Administração.

11.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

11.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência/Projeto Básico, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

11.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

11.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

11.7. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

11.8. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

11.8.1. Em caso de prorrogação da ata, poderá ser renovado o quantitativo originalmente registrado.

12. DA FORMAÇÃO DO CADASTRO RESERVA

12.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

12.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

12.1.2. dos licitantes que mantiverem sua proposta original

12.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

12.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

12.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

12.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

12.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas

condições estabelecidos no edital; ou

12.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

12.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

12.4.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

12.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

13. DOS RECURSOS

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

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

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

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

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

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

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

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

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

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

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

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

13.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.confea.org.br/.

14. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

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

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

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

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

14.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

14.1.2.4. deixar de apresentar amostra; ou

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

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

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

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

14.1.6. fraudar a licitação;

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

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

14.1.7.2. induzir deliberadamente a erro no julgamento;

14.1.7.3. apresentar amostra falsificada ou deteriorada;

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

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

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

14.2.1. advertência;

14.2.2. multa;

14.2.3. impedimento de licitar e contratar e

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

14.3. Na aplicação das sanções serão considerados:

14.3.1. a natureza e a gravidade da infração cometida.

14.3.2. as peculiaridades do caso concreto

14.3.3. as circunstâncias agravantes ou atenuantes

14.3.4. os danos que dela provierem para a Administração Pública

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

14.4. A multa será recolhida no prazo máximo de 15 (quinze) dias úteis, a contar da comunicação oficial.

14.4.1. Para as infrações previstas nos itens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0.5% a 15% do valor do contrato licitado.

14.4.2. Para as infrações previstas nos itens 14.1.4, 14.1.5, 14.1.6, 14.1.7, 14.1.8 e

14.1.9, a multa será de 15% a 30% do valor do contrato licitado.

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

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

14.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 14.1.1, 14.1.2 e 14.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo o qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

14.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 14.1.5, 14.1.6, 14.1.7, 14.1.8 e 14.1.9, bem como pelas infrações administrativas previstas nos itens 14.1.1, 14.1.2, 14.1.3 e 14.1.4, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133, de 2021.

14.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 14.1.4, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

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

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

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

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

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

14.15. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

14.15.1. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no Sicaf serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

15. DA IMPUGNAÇAO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

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

15.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos seguintes meios: e-mail: licitação@confea.org.br

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

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

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

16. DAS DISPOSIÇÕES GERAIS

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

16.2. 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.

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

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

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

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

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

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

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

16.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.confea.org.br

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

16.11.1. Anexo I - Termo de Referência (1514004).

16.11.1.1. Apêndice do Anexo I – Estudo Técnico Preliminar (1478206)

16.11.1.2. Apêndice do Anexo I - Especificação Técnica (1514014)

16.11.1.3. Apêndice do Anexo I - Planilha de Quantitativos e Pesquisa de Preços – ETP /

Registro de Preços (1514034)

16.11.2. Anexo II - Minuta de Ata de Registro de Preços (1487307)

16.11.3. Anexo III - Minuta do Contrato (1487308)

Documento assinado eletronicamente por **João Paulo dos Santos Mouta Cipriano Guimarães**, **Pregoeiro(a)**, em 01/04/2026, às 12:01, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://confea.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1514080** e o código CRC **E97D487E**.

Referência: Processo nº 00.003608/2024-71 SEI nº 1514080

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

TERMO DE REFERÊNCIA SERVIÇOS DE TIC CONFEA-GSI Nº 2/2026

Processo: 00.003608/2024-71
Tipo de Processo: Aquisição/Contratação: Bens ou Serviços
Assunto: Fornecimento de Software/Serviço de Gestão de Vulnerabilidades
Interessado: Setor de Infraestrutura e Arquitetura

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de solução de tecnologia da informação e comunicação para gerenciamento de exposição, compreendendo licenciamento de *software*, serviços especializados, suporte técnico, treinamento e serviços continuados, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. **Quantitativos estimados e identificação dos órgãos participantes:**

1.2.1. Em atendimento ao disposto no art. 6º, inciso XXIII, alínea "d", da Lei nº 14.133/2021, o objeto da presente contratação contempla a definição dos quantitativos estimados de bens e serviços, individualizados por órgão, com base nas manifestações formais de intenção registradas no âmbito da **Intenção de Registro de Preços – IRP nº 00013/2025**.

1.2.2. Os quantitativos foram informados pelos órgãos participantes a partir de seus respectivos planejamentos internos, não constituindo obrigação de contratação integral, nos termos do art. 83 da Lei nº 14.133/2021, destinando-se exclusivamente à formação da Ata de Registro de Preços.

1.2.3. **Órgão Gerenciador - Conselho Federal de Engenharia e Agronomia - Confea**

ITEM	CATSER	DESCRIÇÃO	UNIDADE	QTD TOTAL
1	27464	Licenciamento para a *Gestão de Vulnerabilidades*	UN	580
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	20
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	41
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	480
5	26972	Serviço de Instalação	UN	4
6	3840	Treinamento por Plataforma	UN	4
7	27014	Serviço Continuado para a *Gestão de Vulnerabilidades*	UN	36

1.2.4. **Órgãos Participantes da IRP**

1.2.5. **a) Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome – MDS**

ITEM	CATSER	DESCRIÇÃO	UNIDADE	QTD TOTAL
1	27464	Licenciamento para a *Gestão de Vulnerabilidades*	UN	7600
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	50
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	40
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	6400
5	26972	Serviço de Instalação	UN	4
6	3840	Treinamento por Plataforma	UN	4
7	27014	Serviço Continuado para a *Gestão de Vulnerabilidades*	UN	36

1.2.6. **b) Secretaria de Estado da Educação de Rondônia – SEDUC/RO**

ITEM	CATSER	DESCRIÇÃO	UNIDADE	QTD TOTAL
1	27464	Licenciamento para a *Gestão de Vulnerabilidades*	UN	2900
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	100
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	500
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	19000
5	26972	Serviço de Instalação	UN	4

6	3840	Treinamento por Plataforma	UN	4
7	27014	Serviço Continuado para a *Gestão de Vulnerabilidades*	UN	36

1.2.7. **c) Instituto de Desenvolvimento Florestal e da Biodiversidade do Estado do Pará – IDEFLOR-Bio/PA**

ITEM	CATSER	DESCRIÇÃO	UNIDADE	QTD TOTAL
1	27464	Licenciamento para a *Gestão de Vulnerabilidades*	UN	-
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	60
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	200
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	500
5	26972	Serviço de Instalação	UN	4
6	3840	Treinamento por Plataforma	UN	4
7	27014	Serviço Continuado para a *Gestão de Vulnerabilidades*	UN	36

1.3. **Consolidação dos quantitativos**

1.4. Os quantitativos totais da contratação correspondem à soma das estimativas apresentadas pelo órgão gerenciador e pelos órgãos participantes, conforme planilha consolidada que integra este Termo de Referência como anexo, servindo de base para:

1.4.1. *definição do valor estimado da contratação;*

1.4.2. *julgamento das propostas;*

1.4.3. *formação da Ata de Registro de Preços;*

1.4.4. *futuras contratações pelos órgãos aderentes.*

ITEM	CATSER	DESCRIÇÃO	UNIDADE	QTD TOTAL
1	27464	Licenciamento para a *Gestão de Vulnerabilidades*	UN	11080
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	230
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	781
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	26380
5	26972	Serviço de Instalação	UN	16
6	3840	Treinamento por Plataforma	UN	16
7	27014	Serviço Continuado para a *Gestão de Vulnerabilidades*	UN	144

1.4.5. Os serviços objeto desta contratação são caracterizados como *comuns*, uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

1.4.6. O prazo de vigência da contratação é de 36 (trinta e seis meses) contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

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

1.5. **Classificação do objeto quanto ao modelo de execução**

1.5.1. O objeto da presente contratação caracteriza-se como serviço contínuo, uma vez que envolve a prestação recorrente e permanente de serviços de gestão de vulnerabilidades, monitoramento, suporte técnico especializado e atualização contínua das soluções contratadas, essenciais à manutenção da segurança da informação e à continuidade operacional dos ambientes tecnológicos dos órgãos participantes.

1.6. **Do enquadramento nos arts. 3º e 4º da IN SGD nº 94/2022**

1.6.1. A presente contratação não se enquadra nas vedações previstas no art. 3º da Instrução Normativa SGD nº 94/2022, uma vez que o objeto consiste em uma única solução de TIC, composta por licenciamento, serviços técnicos especializados e suporte operacional, elementos indissociáveis para o funcionamento da solução de Gestão de Exposição/Vulnerabilidades.

1.6.2. Ademais, a contratação não envolve a gestão de processos de TIC ou a gestão da segurança da informação, mas tão somente o fornecimento de ferramenta e apoio técnico especializado, permanecendo sob responsabilidade exclusiva do CONFEA a governança, a tomada de decisão, a fiscalização e a gestão do contrato.

1.6.3. Da mesma forma, não se aplica o disposto no art. 4º da referida Instrução Normativa, uma vez que a contratada não exercerá atividades de avaliação, mensuração ou fiscalização da execução contratual, funções estas atribuídas exclusivamente a servidores designados pela Administração, inexistindo conflito de interesses.

1.7. **Do enquadramento nos art. 5º da IN SGD nº 94/2022**

1.7.1. A Administração certifica que, na elaboração do Termo de Referência e de seus anexos, foram observadas as vedações previstas no art. 5º da Instrução Normativa SGD nº 94/2022, não havendo previsão de exigências restritivas à competitividade, direcionamento tecnológico, delegação de atividades de gestão ou fiscalização, nem qualquer outra hipótese vedada pela referida norma.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

2.1. A descrição da solução como um todo encontra-se *pormenorizada* em tópico específico do Estudo Técnico Preliminar - apêndice deste Termo de Referência.

2.2. A solução de TIC consiste em ferramenta de Gestão de Exposição/Vulnerabilidades que possibilite à instituição identificar, analisar, priorizar e tratar vulnerabilidades de forma contínua, visando a proteção de ativos de informação críticos, a mitigação de riscos cibernéticos e a conformidade com normativos legais e regulatórios (LGPD, Decreto nº 9.637/2018 - Política Nacional de Segurança da Informação, normas ISO/IEC 27001 e 27002, dentre outros).

2.3. A crescente complexidade dos ambientes de Tecnologia da Informação e Comunicação - TIC, associada ao aumento no volume e na sofisticação de ameaças cibernéticas, torna inviável a execução manual e descentralizada da identificação e tratamento de vulnerabilidades. Uma ferramenta especializada se faz necessária para automatizar processos, gerar relatórios gerenciais e técnicos, apoiar a governança e fornecer subsídios para auditorias internas e externas, além de responder a recomendações de órgãos de controle.

2.4. A solução contratada deverá contemplar os seguintes bens e serviços, em quantitativo compatível com a realidade da instituição:

2.4.1. *Licenciamento* de ferramenta de *gestão de vulnerabilidades* com validade de 36 meses;

2.4.2. *Licenciamento* de ferramenta de *gestão de vulnerabilidades* para *aplicações web* com 36 meses de validade;

2.4.3. *Licenciamento* de ferramenta de *gestão de superfície de ataque* com validade de 36 meses;

2.4.4. *Licenciamento* de ferramenta para *gestão de vulnerabilidades* para *Active Directory* com 36 meses de validade;

2.4.5. Serviço de instalação especializada por plataforma;

2.4.6. Treinamento das ferramentas por módulo;

2.4.7. Serviço continuado para *gestão de vulnerabilidades* com 36 meses de vigência.

2.5. O quantitativo ora especificado tem como objetivo assegurar cobertura integral dos ativos mapeados, a autonomia da equipe técnica na operação e a continuidade do serviço de gestão de vulnerabilidades, garantindo assim a efetividade da solução ao longo do período contratual.

2.6. ***Os quantitativos estimados da presente contratação foram definidos a partir da Intenção de Registro de Preços regularmente instaurada, considerando as manifestações formais de interesse apresentadas pelos órgãos participantes, bem como a necessidade estimada do órgão gerenciador, nos termos do Decreto nº 11.462, de 31 de março de 2023.***

2.7. DAS ESPECIFICAÇÕES TÉCNICAS

2.7.1. As especificações técnicas de todos os Itens se encontram no **Anexo I** deste Termo de Referência. (1448313)

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. NECESSIDADES DE NEGÓCIO

3.2. Os ataques contra sistemas de informação têm se tornado cada vez mais frequentes e sofisticados em todo o mundo, e no Conselho Federal de Engenharia e Agronomia (Confea) não é diferente. A tendência observada no cenário global indica que tanto a quantidade quanto a severidade dessas ocorrências irão aumentar de forma expressiva nos próximos anos, ampliando significativamente a superfície de risco a que estão submetidas as organizações públicas e privadas.

3.3. Nesse contexto, a *cibersegurança* deixou de ser apenas uma prática recomendada e tornou-se um requisito estratégico para a continuidade das operações institucionais. As ameaças evoluíram além dos métodos clássicos - como *phishing*, *malwares* e *vírus* de propagação simples - para incluir ataques cada vez mais complexos, como a exploração de vulnerabilidades *zero-day* em *softwares*, campanhas de engenharia social altamente direcionadas e ações de *ransomware*, que sequestram dados críticos mediante pedido de resgate. Tais cenários evidenciam que proteger apenas a camada perimetral já não é suficiente: é imprescindível adotar práticas estruturadas de *Gestão de Vulnerabilidades*, capazes de identificar, priorizar e corrigir falhas antes que estas sejam exploradas por agentes maliciosos.

3.4. Para garantir a integridade, a confidencialidade e a disponibilidade das informações, bem como a

continuidade dos negócios, o Confea mantém um Sistema de Gestão de Segurança da Informação (SGSI), que contempla a definição de papéis, responsabilidades, políticas, normas e procedimentos de segurança de TIC. Esse sistema pressupõe, entre outras medidas, o monitoramento constante, a realização de testes periódicos e a implementação de ações corretivas diante de incidentes ou deficiências identificadas. Dentro desse escopo, o processo de *Gestão de Vulnerabilidades* desponta como um dos pilares mais relevantes, pois permite a antecipação e mitigação de riscos em um ambiente de ameaças cibernéticas em constante transformação.

3.5. A implementação desse processo envolve diferentes etapas: inicia-se pela identificação de ativos de TI - servidores físicos e virtuais, estações de trabalho, *notebooks*, dispositivos móveis, *appliances* de segurança, equipamentos de rede (*switches*, roteadores, *firewalls*), bancos de dados, *aplicações web*, sistemas críticos, entre outros. No caso do Confea, o parque tecnológico conta atualmente com mais de 700 ativos de diferentes naturezas, o que torna o ambiente altamente dinâmico, interconectado e complexo de gerenciar. Essa complexidade acarreta enormes desafios, sobretudo na detecção e tratamento de vulnerabilidades técnicas que surgem continuamente devido a fatores como:

3.5.1. falhas de configuração;

3.5.2. ausência de *patch management* adequado;

3.5.3. *bugs* de *software* não corrigidos;

3.5.4. portas e serviços expostos indevidamente;

3.5.5. uso de credenciais fracas;

3.5.6. ambientes legados e desatualizados;

3.5.7. entre outras fragilidades.

3.6. Para enfrentar esse cenário, as ferramentas automatizadas de *scanner* de vulnerabilidades desempenham papel central, pois realizam varreduras abrangentes em busca de brechas de segurança, analisando códigos, configurações e comunicações de rede. Essas soluções permitem identificar rapidamente vulnerabilidades conhecidas em grande escala, fornecendo uma visão ampla do nível de exposição e facilitando a tomada de decisões proativas para mitigação.

3.7. Após a identificação das vulnerabilidades, torna-se essencial avaliar o risco associado a cada uma delas. Esse processo de análise considera fatores como:

3.7.1. impacto potencial sobre os ativos e serviços críticos;

3.7.2. probabilidade de exploração por agentes de ameaça;

3.7.3. recursos disponíveis para a mitigação.

3.8. Com base nessa avaliação, é possível priorizar correções de forma racional, destinando esforços primeiro às vulnerabilidades mais críticas. As medidas de mitigação podem incluir a aplicação de *patches* de segurança, ajustes de configuração, atualizações de *software* ou ainda a implementação de controles compensatórios quando a correção imediata não for possível.

3.9. Entretanto, a *Gestão de Vulnerabilidades* não se encerra com a correção inicial. É indispensável verificar a efetividade das medidas adotadas, monitorar continuamente o ambiente e realizar revisões periódicas do processo, de modo a identificar oportunidades de melhoria e garantir sua eficácia contínua. Dessa forma, a gestão de vulnerabilidades deve ser entendida como um ciclo permanente e iterativo, que acompanha a evolução tecnológica e as mudanças no panorama das ameaças cibernéticas.

3.10. Além das boas práticas de governança em segurança, o Confea fundamenta suas ações em normativos legais e regulatórios vigentes, com destaque para a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que estabelece princípios e obrigações para o tratamento seguro das informações pessoais. O alinhamento à LGPD e a outros normativos governamentais reforça a necessidade de processos estruturados de prevenção, capazes de reduzir a exposição a incidentes e assegurar o cumprimento das obrigações legais.

3.11. Assim, a contratação de uma solução de *Gestão de Vulnerabilidades* justifica-se como medida essencial para fortalecer a postura de segurança do Confea, assegurando a proteção dos ativos institucionais, a conformidade legal e regulatória, a redução de riscos e a preservação da confiança dos usuários internos e externos na integridade dos serviços prestados.

3.12. **NECESSIDADES TÉCNICAS**

3.13. A solução a ser contratada deve possibilitar a gestão contínua de vulnerabilidades e da exposição a ameaças, de forma proativa e recorrente. Isso implica a adoção de práticas sistemáticas de identificação, avaliação, categorização, priorização, tratamento e análise crítica das vulnerabilidades e riscos de segurança que afetam os ativos corporativos de Tecnologia da Informação e Comunicação (TIC). A abordagem deve abranger tanto o gerenciamento da superfície de ataque interna e externa quanto a análise de exposição a

ameaças, permitindo uma visão integrada do nível de risco cibernético da instituição.

3.14. Para atingir esse objetivo, torna-se imprescindível a utilização de ferramenta especializada capaz de:

3.14.1. realizar varreduras e avaliações abrangentes de vulnerabilidades;

3.14.2. verificar a conformidade das configurações de ativos de acordo com normas e padrões reconhecidos;

3.14.3. fornecer mecanismos de priorização de riscos que orientem a tomada de decisão gerencial.

3.15. Descoberta e identificação de ativos;

3.16. A solução deve realizar a descoberta automática e a identificação detalhada dos ativos presentes no ambiente corporativo do Confea, analisando suas configurações sob os critérios de segurança, conformidade e aderência a normas, *frameworks* e bases de conhecimento internacionalmente reconhecidos. Além disso, deve possibilitar o estabelecimento de linhas de base de configuração, permitindo o rastreamento de alterações e a detecção de desvios que possam comprometer a segurança.

3.17. Amplitude de cobertura;

3.18. O processo de *Gestão de Vulnerabilidades* deve abranger de forma ampla os ativos de TIC da instituição, incluindo:

3.18.1. dispositivos de usuário final (estações de trabalho, *notebooks*, periféricos e dispositivos móveis);

3.18.2. dispositivos de rede (*switches*, roteadores, *firewalls* e *appliances* de segurança);

3.18.3. dispositivos inteligentes conectados à rede, como relógios de ponto eletrônico e outros equipamentos de Internet das Coisas – IoT;

3.18.4. servidores físicos e virtuais, contêineres e sistemas operacionais;

3.18.5. aplicações corporativas e serviços em rede;

3.18.6. ativos e posturas de segurança em ambientes de nuvem.

3.19. A diversidade e heterogeneidade do parque tecnológico do Confea demandam uma solução que consiga atuar de forma transversal, contemplando desde a camada de usuário até a infraestrutura crítica.

3.20. Varreduras de vulnerabilidade;

3.21. Devem ser realizadas varreduras automatizadas de vulnerabilidades em ativos internos e externos com periodicidade mínima trimestral, incluindo a repetição das varreduras após a aplicação de patches, atualizações e demais salvaguardas.

3.22. As varreduras devem contemplar tanto abordagens autenticadas quanto não autenticadas, garantindo profundidade e abrangência.

3.23. A solução deve apresentar compatibilidade, no mínimo, com o protocolo *Security Content Automation Protocol* – SCAP, de modo a assegurar padronização e confiabilidade.

3.24. Quando devidamente calibradas, as varreduras automatizadas conduzidas por agentes e pela rede externa devem ter como meta a periodicidade diária, enquanto as varreduras da rede interna devem ocorrer em ciclos mensais ou quinzenais, observando-se os períodos de gestão de patches e os impactos em desempenho, disponibilidade e tráfego de rede.

3.25. Priorização baseada em risco;

3.26. A ferramenta deve incluir tecnologia de *Vulnerability Prioritization Technology* (VPT), baseada em risco e altamente adaptável. Essa priorização deve levar em consideração, de forma combinada:

3.26.1. a severidade das vulnerabilidades identificadas;

3.26.2. a criticidade dos ativos e serviços afetados;

3.26.3. o contexto dinâmico das ameaças (existência e atividade de *exploits*).

3.27. Esse modelo de priorização orienta a destinação de esforços para as vulnerabilidades que representam maior risco efetivo ao negócio, otimizando recursos e fortalecendo a resiliência organizacional.

3.28. Integração com inteligência de ameaças;

3.29. A solução deve agregar recursos de *Threat Intelligence*, permitindo o rastreamento do uso ativo de vulnerabilidades e sua priorização com base em diferentes níveis de inteligência:

3.29.1. estratégico: relatórios, bases de conhecimento e fontes abertas, incluindo *Deep Web e Dark Web;*

3.29.2. tático: correlação com táticas, técnicas e procedimentos (TTPs) de adversários;

3.29.3. operacional: correlação com indicadores de comprometimento (IOCs).

3.30. A inteligência de ameaças deve ser proveniente tanto do fabricante da ferramenta quanto de fontes abertas e, adicionalmente, da própria contratada, ampliando a qualidade e diversidade das informações utilizadas no processo decisório.

3.31. Acompanhamento de referências e melhores práticas;

3.32. A solução deve contemplar o acompanhamento constante de alertas de segurança, atualizações, referenciais de vulnerabilidades e boas práticas de *hardening* para ativos de TIC, com base em repositórios e padrões amplamente reconhecidos, tais como:

3.32.1. *NIST National Vulnerability Database* (NVD);

3.32.2. *MITRE Common Vulnerabilities and Exposures* (CVE);

3.32.3. *NIST Official Common Platform Enumeration* (CPE);

3.32.4. *MITRE Common Weakness Enumeration* (CWE);

3.32.5. *OWASP Top 10*;

3.32.6. *CIS Benchmarks*.

3.33. Além disso, devem ser considerados os repositórios e centros de segurança dos principais fabricantes de tecnologia aplicáveis aos ativos do Confea, contemplando no mínimo: Microsoft, Oracle, Google, Red Hat, Dell/EMC, HP/Aruba, Check Point, F5 Networks, Broadcom/Symantec, VMware, Micro Focus, Commvault, Cisco, Mozilla e Adobe.

3.34. **ADERÊNCIA NORMATIVA**

3.35. O objeto da contratação está previsto no Plano de Contratações Anual, Processo 00.000457/2025-81, Decisão Plenária nº PL-2351/2024, conforme detalhamento a seguir:

I - ID PCA no PNCP: GND, Outras Despesas Correntes, Serviços de Terceiros, Serviços de Informática. (1125251)

3.36. O objeto da contratação também está alinhado com a Estratégia de Governo Digital e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) *2023-2025* do *Confea*, conforme demonstrado abaixo:

3.36.1. A contratação de solução para gestão de vulnerabilidades está alinhada às diretrizes gerais do Plano Diretor de Tecnologia da Informação (PDTI) do Confea, em especial aquelas voltadas ao fortalecimento da governança, à segurança da informação e à melhoria contínua da infraestrutura tecnológica. O PDTI 2023-2025 estabelece, entre suas prioridades, a adoção de um modelo de governança baseado em melhores práticas de mercado, a busca por aumento de produtividade, a garantia de segurança da informação e a valorização dos recursos humanos da área de TI.

3.36.2. Nesse sentido, a presente contratação contribui de forma transversal e estruturante para diversas iniciativas em curso, ao prover um mecanismo que fortalece a visibilidade, a resiliência e a conformidade do ambiente tecnológico. A solução de gestão de vulnerabilidades atua como elemento de suporte crítico para a consecução de objetivos estratégicos previstos, tais como:

3.36.2.1. ID 18 – Reestruturação dos servidores de *Active Directory*. A identificação e mitigação de vulnerabilidades em controladores de domínio é condição indispensável para assegurar que a reestruturação dos servidores de *Active Directory* se dê em ambiente confiável, reduzindo riscos decorrentes de objetos legados e conflitos existentes.

3.36.2.2. ID 23 – *Security Operations Center* (SOC). A gestão de vulnerabilidades complementa a atuação do SOC ao fornecer insumos qualificados sobre exposição a riscos, ampliando a capacidade de correlação de eventos e priorização de incidentes.

3.36.2.3. ID 25 – Solução de avaliação e tratamento de dados (LGPD). O processo de gestão de vulnerabilidades reforça a conformidade com a LGPD, na medida em que reduz o risco de incidentes de segurança que possam comprometer a confidencialidade, a integridade e a disponibilidade de dados pessoais.

3.36.2.4. ID 27 – Solução de inventário e gerenciamento de *endpoints*. A descoberta contínua e ativa de ativos de TI, inerente ao processo de gestão de vulnerabilidades, converge com a necessidade de inventário e gerenciamento de *endpoints*, fornecendo informações que subsidiam a adoção de tecnologia específica para esse fim.

3.37. Assim, a contratação ora proposta não apenas observa as diretrizes do PDTI 2023-2025 como também se integra a diferentes iniciativas estratégicas, atuando como fator de sustentação e catalisador para sua efetiva implementação. Com isso, reforça-se a coerência do planejamento de TI do Confea, assegurando que os investimentos realizados sejam convergentes e que os riscos de segurança cibernética sejam tratados de maneira sistêmica e coordenada.

4. REQUISITOS DA CONTRATAÇAO

4.1. Requisitos de Negócio:

4.2. a) Objetivo de negócio;

4.2.1. Dotar o Contratante de uma solução integrada de *Gestão de Vulnerabilidades* que forneça visibilidade contínua e em tempo quase real do risco cibernético, priorize correções com base em criticidade do ativo e ameaça, e sustente a continuidade dos serviços públicos digitais, a conformidade regulatória e a tomada de decisão pela TI.

4.3. b) Escopo de negócio (itens do objeto);

4.3.1. Item 1 – Gestão de Vulnerabilidades (36 meses): varredura autenticada/sem agente; priorização por CVSS e inteligência de ameaças; RBAC; APIs; relatórios (HTML/PDF/CSV); inventário e painéis centralizados; suporte a ambientes *on-prem* e nuvem (AWS/Azure/GCP).

4.3.2. Item 2 – Gestão de Vulnerabilidades para Aplicações Web (DAST): cobertura OWASP Top 10; escopos por IP/FQDN; autenticação (básica, NTLM, formulário, cookies, Selenium, Bearer); *crawler* customizável; limites e políticas de varredura; evidências detalhadas.

4.3.3. Item 3 – Gestão de Superfície de Ataque Externa (EASM): descoberta/mapeamento de ativos expostos; correlação com CVE/NVD; integração com Cloudflare/AWS/Azure/GCP; relatórios e trilhas de auditoria.

4.3.4. Item 4 – Gestão de Vulnerabilidades para Active Directory/Entra ID: descoberta de fraquezas/configurações; correlação MITRE ATT&CK; monitoramento contínuo; *dashboards*; gestão de risco de identidades.

4.3.5. Item 5 – Serviço de Instalação: arquitetura, configuração, testes de aceitação e documentação (*as-built*, POPs).

4.3.6. Item 6 – Treinamento por plataforma: até 4 participantes/turma; 16 horas por solução; remoto e síncrono.

4.3.7. Item 7 – Serviço Continuado (36 meses, 24x7x365): suporte proativo/reativo; SLA de atendimento em até 2h; acompanhamento de saúde do ambiente e evolução do risco.

4.4. c) Benefícios e valor esperado;

4.4.1. Redução do tempo de detecção, priorização e remediação de vulnerabilidades.

4.4.2. Visão única e centralizada de exposição por ativo, área e tecnologia, incluindo AD e *aplicações web*.

4.4.3. Integração com SIEM/ITSM/CMDB e automação por API para acelerar *workflows*.

4.4.4. Conformidade com boas práticas (ISO 27001/27002), LGPD e diretrizes E-Ciber/TCU.

4.4.5. Capacitação da equipe e transferência de conhecimento para operação cotidiana.

4.5. d) Unidades de fornecimento e vigência;

4.5.1. Item 1: licenças por ativo/dispositivo de rede – vigência de 36 meses.

4.5.2. Item 2: licenças por site/FQDN – 36 meses.

4.5.3. Item 3: licenças por 2 ativos externos por unidade – 36 meses.

4.5.4. Item 4: licenças por 2 usuários AD por unidade – 36 meses.

4.5.5. Itens 5, 6 e 7: serviços associados à implantação, treinamento e operação continuada.

4.6. e) Resultados mínimos (*outcomes*) de negócio;

4.6.1. Cobertura de varreduras periódicas (agendadas) em todo o parque crítico com *dashboards* e relatórios gerenciais/técnicos.

4.6.2. Priorização baseada em criticidade do ativo + ameaça (idade, exploração ativa, *exploit* disponível etc.).

4.6.3. Descoberta contínua de ativos (*on-prem*, nuvem e externos) e inventário consolidado.

4.6.4. Monitoramento e análise de ataques com mapeamento MITRE ATT&CK e evidências.

4.6.5. Relatórios semestrais (ou sob demanda) com panorama de vulnerabilidades e medidas adotadas.

4.7. f) Indicadores de desempenho (nível de negócio);

4.7.1. % de ativos críticos com *scan* autenticado recente.

4.7.2. Tempo médio para correção (MTTR) por severidade.

4.7.3. Tendência de exposição cibernética por área/organização.

4.7.4. Cobertura de aplicações web no escopo e redução de achados OWASP Top 10.

4.7.5. Eventos/anomalias em AD identificados e remediados.

4.7.6. Cumprimento dos SLAs de atendimento do serviço continuado.

4.8. g) Requisitos de integração e interoperabilidade (vista de negócio);

4.8.1. Integração via APIs REST com SIEM, ITSM e CMDB, além de diretórios (AD/LDAP) e provedores de nuvem.

4.8.2. Exportação de dados e portabilidade (HTML, PDF, CSV/JSON) para relatórios e auditorias.

4.8.3. Gestão centralizada de scanners, sensores e agentes em uma única console.

4.9. h) Restrições e condições operacionais;

4.10. Operação com baixa intervenção manual, com agendamento automático e correlação inteligente.

4.10.1. Acesso multiusuário (mín. 10 sessões) com RBAC e trilhas de auditoria.

4.10.2. Disponibilização da solução em SaaS, nuvem ou *on-premises* conforme contexto do Contratante.

4.10.3. Para SaaS, observância às exigências de hospedagem e cópias em território nacional conforme normativo citado.

4.11. i) Entregáveis de negócio;

4.11.1. Plano de instalação/arquitetura e relatório *as-built* (diagramas lógicos/físicos, quando couber).

4.11.2. Perfis de varredura por criticidade, políticas e janelas de escaneamento.

4.11.3. Relatórios gerenciais e técnicos recorrentes e sob demanda.

4.11.4. Materiais de treinamento e registro de participação.

4.11.5. Relatórios semestrais do serviço continuado com tendências e recomendações.

4.12. j) Critérios de aceite (nível de negócio);

4.12.1. Conclusão da implantação com varreduras executadas e consoles operacionais.

4.12.2. Disponibilização de *dashboards* e relatórios previstos.

4.12.3. Execução de testes de validação (detecção de vulnerabilidades conhecidas, desempenho, falsos positivos) e documentação entregue.

4.13. **Requisitos de Capacitação**

4.14. a) Capacitação da Equipe Técnica (Contratante);

4.14.1. Treinamento remoto, síncrono, com carga mínima de 16 horas por solução contratada (Itens 1, 2, 3 ou 4).

4.14.2. Cada turma deve ter até 4 participantes, garantindo atenção individualizada.

4.14.3. Conteúdo obrigatório:

4.14.4. Arquitetura e componentes da solução.

4.14.5. Modalidades e topologias de varredura de vulnerabilidades.

4.14.6. Configuração da console, serviços de rede e *backup* de configurações.

4.14.7. Depuração, troubleshooting e abertura de chamados.

4.14.8. Gerenciamento de licenças, relatórios e *dashboards*.

4.14.9. Profissionais treinados devem ser capazes de operar a solução, interpretar relatórios e integrar os resultados às atividades de segurança do Contratante.

4.15. b) Capacitação da Equipe Técnica (Contratada);

4.15.1. A instalação e o serviço continuado devem ser realizados por profissionais certificados nas soluções fornecidas.

4.15.2. A contratada deve comprovar experiência prévia em ferramentas de gestão de vulnerabilidades e apresentar certificações técnicas aplicáveis.

4.15.3. O serviço continuado (24x7x365) deve ser prestado por equipe capacitada para suporte proativo e reativo, com capacidade de interação direta com fabricantes.

4.16. c) Transferência de Conhecimento;

4.16.1. Durante a implantação e configuração, a contratada deve repassar conhecimentos à equipe do Contratante por meio de sessões práticas.

4.16.2. Ao final do treinamento, deve ser disponibilizado material didático (slides, manuais ou apostilas) e, quando possível, gravação das sessões.

4.16.3. A contratada deve oferecer recomendações de boas práticas para gestão diária da solução, integração com sistemas existentes e adoção de novos recursos.

4.17. d) Objetivo de Capacitação;

4.17.1. Garantir que a equipe interna do Contratante tenha condições de operar, administrar e evoluir a solução contratada sem dependência excessiva da contratada, exceto para suporte especializado e atualizações críticas.

4.18. **Requisitos Legais**

4.19. a) A contratação deverá observar a legislação vigente sobre contratações públicas, em especial:

4.19.1. Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos).

4.19.2. Lei nº 13.709/2018 – LGPD (Lei Geral de Proteção de Dados Pessoais).

4.19.3. Lei nº 12.965/2014 – Marco Civil da Internet.

4.19.4. Lei nº 12.846/2013 – Lei Anticorrupção.

4.19.5. Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética – E-Ciber).

4.20. b) Normativos Infralegais e Orientações Técnicas;

4.20.1. IN SGD/ME nº 94/2022 – sobre planejamento da contratação de TIC.

4.20.2. IN SGD/ME nº 05/2021, art. 18 – obrigatoriedade de armazenamento de dados em território nacional para serviços em nuvem/SaaS.

4.20.3. Portaria SGD/MGI nº 5.950/2023, quando aplicável à métrica de unidades de serviço em nuvem (USN).

4.20.4. Orientações do Tribunal de Contas da União (TCU), especialmente sobre contratação de TIC, gestão de riscos e avaliação de propostas exequíveis.

4.21. c) Normas Técnicas e de Boas Práticas;

4.21.1. ISO/IEC 27001 e 27002 – Sistema de Gestão de Segurança da Informação.

4.21.2. NIST Cybersecurity Framework – práticas de segurança reconhecidas internacionalmente.

4.21.3. CIS Benchmarks e DISA STIGs – referências para auditoria de configuração.

4.21.4. PCI DSS – quando envolver aplicações e dados relacionados a transações financeiras.

4.22. d) Condições Contratuais;

4.22.1. Todas as licenças deverão ser emitidas em nome do Contratante, não sendo aceitas licenças de prestadores de serviço.

4.22.2. O contrato deverá prever cláusula de reversibilidade, assegurando ao Contratante o direito de exportar e portar todos os dados e históricos em formato aberto (CSV, JSON, PDF).

4.22.3. A contratada deve cumprir a responsabilidade legal como operadora de dados (art. 39 da LGPD), com obrigação de confidencialidade e de reporte imediato de incidentes de segurança.

4.22.4. É vedado à contratada armazenar, compartilhar ou transferir informações do Contratante para terceiros sem autorização expressa.

4.23. e) Garantia de Conformidade;

4.23.1. A solução deve atender às disposições de segurança, disponibilidade e soberania dos dados, incluindo cópia de segurança mantida em território brasileiro, quando em nuvem.

4.23.2. A contratada deverá manter registros para fins de auditoria e responsabilização, conforme previsto em lei.

4.23.3. O contrato deverá prever penalidades administrativas pelo não cumprimento dos requisitos legais e normativos.

4.24. **Requisitos de Manutenção**

4.25. a) Manutenção da Solução (Software e Licenciamento);

4.25.1. Todas as licenças contratadas terão vigência mínima de 36 (trinta e seis) meses, cobrindo atualizações de versão, patches de segurança e novas funcionalidades disponibilizadas pelo fabricante.

4.25.2. A contratada deverá garantir a aplicação tempestiva de atualizações e correções, incluindo *hotfixes*

críticos.

4.25.3. As atualizações não poderão gerar custos adicionais além do valor contratado.

4.26. b) Serviço Continuado de Manutenção (Item 7);

4.26.1. O serviço será prestado na modalidade 24x7x365, com SLA de atendimento de até 2 horas após a solicitação.

4.26.2. A contratada deverá atuar de forma proativa (prevenção, ajustes, acompanhamento de novas vulnerabilidades) e reativa (correção, suporte técnico, incidentes).

4.26.3. O suporte será remoto e síncrono, podendo ser presencial mediante solicitação do Contratante.

4.26.4. O serviço será prestado por profissional certificado na solução, com capacidade de contato direto com o fabricante.

4.27. c) Escopo das Atividades de Manutenção;

4.27.1. Auxílio contínuo em ajustes de perfis de varredura, políticas de risco e regras de correlação.

4.27.2. Aplicação e validação de atualizações de software e novos recursos.

4.27.3. Monitoramento da exposição cibernética do Contratante e indicação de ativos críticos.

4.27.4. Avaliação de indicadores de exposição, evolução de risco e cobertura de ativos críticos.

4.27.5. Validação da efetividade das ações de remediação adotadas pela equipe do Contratante.

4.27.6. Emissão de relatórios periódicos (mínimo semestrais) sobre panorama de vulnerabilidades, ações de contorno e topologia de vetores de ataque.

4.28. d) Documentação e Registro;

4.28.1. Todas as atividades de manutenção deverão ser registradas em relatórios técnicos, incluindo data, hora, responsável, procedimento executado e resultado.

4.28.2. A contratada deverá manter histórico de versões aplicadas, vulnerabilidades críticas atendidas e indicadores de desempenho.

4.29. e) Continuidade e Evolução;

4.29.1. A contratada deve garantir que a solução permaneça operante, segura e aderente aos normativos vigentes ao longo do contrato.

4.29.2. Caso ocorram mudanças relevantes na solução (arquitetura, APIs, recursos), a contratada deverá prover ajustes necessários para manter a operação do Contratante sem custos adicionais.

4.29.3. Deverá ser assegurada a compatibilidade com integrações existentes (SIEM, ITSM, AD, nuvem) após cada atualização.

4.30. **Requisitos Temporais**

4.31. a) Vigência das Licenças;

4.31.1. Todos os licenciamentos contratados (Itens 1, 2, 3 e 4) deverão ter duração mínima de 36 (trinta e seis) meses, contados a partir da ativação e aceite formal pelo Contratante.

4.32. b) Serviços de Instalação e Implantação (Item 5);

4.32.1. A instalação, configuração e testes de aceitação deverão ser concluídos em prazo a ser definido no plano de instalação, aprovado pelo Contratante antes do início dos trabalhos.

4.32.2. O prazo máximo de instalação e entrega da solução deverá observar o cronograma acordado, contemplando fases, marcos e responsáveis.

4.33. c) Treinamento (Item 6);

4.33.1. O treinamento deverá ser ministrado imediatamente após a instalação, garantindo que a equipe do Contratante esteja apta a operar a solução desde a entrada em produção.

4.33.2. Cada sessão terá 16 horas de duração mínima, podendo ser dividida em 2 a 4 dias consecutivos ou em cronograma previamente acordado.

4.34. d) Serviço Continuado (Item 7);

4.34.1. O atendimento contínuo deverá ser prestado durante 36 meses ininterruptos, na modalidade 24x7x365.

4.34.2. O SLA de resposta será de até 2 horas após a abertura da solicitação, observado o nível de criticidade.

4.34.3. Relatórios de evolução de vulnerabilidades e exposição cibernética deverão ser entregues

semestralmente ou mediante solicitação do Contratante.

4.35. e) Atualizações e Correções

4.35.1. A aplicação de patches críticos deverá ocorrer em até 24 horas após sua disponibilização pelo fabricante.

4.35.2. Novas versões da solução deverão ser disponibilizadas dentro da vigência contratual, sem custos adicionais, sempre que lançadas oficialmente.

4.36. f) Validade Contratual

4.36.1. O contrato deverá assegurar a execução de todos os serviços e fornecimentos pelo período de 36 meses, com possibilidade de renovação nos termos da legislação vigente.

4.37. **Requisitos de Segurança e Privacidade**

4.38. a) Proteção dos Dados e Informações

4.38.1. Todos os dados, resultados de varreduras, relatórios e informações tratadas pela solução deverão ser criptografados em trânsito e em repouso.

4.38.2. Para soluções em modelo SaaS, deverá ser cumprido o Art. 18 da IN SGD/ME nº 05/2021, garantindo que dados e *metadados* sejam hospedados em território nacional, com pelo menos uma cópia atualizada de segurança no Brasil.

4.38.3. É vedada a utilização de dados do Contratante para qualquer outra finalidade que não a execução do contrato.

4.39. b) Controle de Acesso

4.39.1. A solução deverá implementar controle de acesso baseado em perfis (RBAC), permitindo a segregação de funções entre administradores, analistas e auditores.

4.39.2. O acesso deverá ser protegido por autenticação forte, suportando MFA (Multi-Factor Authentication), SAML e integração com Single Sign-On (SSO).

4.39.3. Será obrigatório o registro e rastreabilidade de todas as ações de usuários, com trilhas de auditoria exportáveis.

4.40. c) Conformidade Normativa

4.40.1. A solução deverá estar alinhada com a LGPD (Lei nº 13.709/2018), com definição clara de papéis (controlador e operador), retenção e descarte seguro de dados.

4.40.2. A solução deve estar aderente a normas de referência em segurança da informação, como ISO/IEC 27001 e 27002, NIST Cybersecurity Framework e CIS Benchmarks.

4.40.3. O tratamento de vulnerabilidades deverá observar as diretrizes da Estratégia Nacional de Segurança Cibernética (E-Ciber) e recomendações do TCU.

4.41. d) Garantia de Confidencialidade e Integridade

4.41.1. A contratada deverá assinar termo de confidencialidade, garantindo a proteção das informações do Contratante.

4.41.2. Deverão ser adotados mecanismos de proteção contra manipulação indevida de relatórios, falsificação de resultados ou acesso não autorizado.

4.41.3. Todos os acessos administrativos à solução deverão ser registrados com data, hora, origem e identidade do usuário.

4.42. e) Gestão de Incidentes de Segurança

4.42.1. A contratada deverá notificar imediatamente o Contratante em caso de incidente de segurança que envolva os dados ou serviços contratados.

4.42.2. Deverá ser garantido o suporte técnico especializado para resposta a incidentes e mitigação de falhas críticas.

4.42.3. Relatórios de incidentes deverão ser disponibilizados ao Contratante, com registro das medidas corretivas e preventivas aplicadas.

4.43. f) Continuidade e Disponibilidade Segura

4.43.1. A solução deverá operar com alta disponibilidade, assegurando redundância e tolerância a falhas.

4.43.2. Backups dos dados e configurações deverão ser executados regularmente, conforme política acordada.

4.43.3. A solução deve permitir plano de reversibilidade, com exportação integral de dados em formatos

abertos (CSV, JSON, PDF).

4.44. **Requisitos Sociais, Ambientais e Culturais**

4.45. a) Requisitos Sociais

4.45.1. A contratação deve observar os princípios da responsabilidade social e da inclusão, assegurando igualdade de condições entre os concorrentes.

4.45.2. É vedada qualquer prática discriminatória no fornecimento dos serviços, devendo a contratada cumprir integralmente a legislação trabalhista e previdenciária vigente.

4.45.3. O serviço deverá ser executado em conformidade com as normas de saúde e segurança do trabalho, garantindo condições adequadas às equipes envolvidas.

4.46. b) Requisitos Ambientais

4.46.1. A solução, preferencialmente na modalidade SaaS ou hospedada em nuvem, deve priorizar *data centers* que adotem práticas de eficiência energética e sustentabilidade ambiental, tais como o uso de energia renovável e programas de neutralização de carbono.

4.46.2. Recomenda-se que a contratada apresente certificações ou evidências de que os ambientes de hospedagem ou de suporte seguem padrões ambientais reconhecidos (ex.: ISO 14001 ou equivalentes).

4.46.3. A contratação deve incentivar a redução do consumo de papel, priorizando relatórios eletrônicos em formatos digitais (HTML, PDF, CSV).

4.47. c) Requisitos Culturais e Éticos

4.47.1. O contrato deverá estar alinhado com os princípios da ética, integridade e transparência administrativa, conforme a Lei Anticorrupção (Lei nº 12.846/2013).

4.47.2. A contratada deverá garantir a promoção de uma cultura de segurança da informação, contribuindo para a conscientização do corpo técnico do Contratante por meio de treinamentos, relatórios claros e linguagem acessível.

4.47.3. Deverá ser respeitada a diversidade cultural e a promoção da cidadania digital, considerando a relevância da segurança cibernética para a sociedade.

4.48. **Requisitos da Arquitetura Tecnológica**

4.49. a) Modelos de Disponibilização

4.49.1. A solução deverá ser disponibilizada em um dos seguintes modelos:

4.49.2. *SaaS* (Software como Serviço), em conformidade com o Art. 18 da IN SGD/ME nº 05/2021.

4.49.3. Hospedagem em nuvem, com requisitos de segurança, soberania e escalabilidade.

4.49.4. Instalação *on-premises*, em infraestrutura do Contratante.

4.50. b) Arquitetura da Solução

4.50.1. A arquitetura deverá permitir gestão centralizada, com console única para administração de *scanners*, agentes e sensores.

4.50.2. A solução deve suportar *multi-tenancy* lógico, permitindo segregação por áreas, redes ou grupos de ativos.

4.50.3. Deverá contemplar descoberta, inventário, varredura, priorização, correlação e relatórios de forma integrada.

4.50.4. Todos os módulos e componentes necessários deverão estar incluídos na entrega (*turn-key*).

4.51. c) Integrações e Interoperabilidade

4.51.1. A solução deve disponibilizar API RESTful com métodos GET, POST, PUT e DELETE.

4.51.2. Deve permitir integração com linguagens como Python, PowerShell, Ruby, Java, JavaScript, PHP e Swift.

4.51.3. Integração nativa ou via API com:

4.51.4. SIEMs para correlação de eventos.

4.51.5. ITSM/CMDB para abertura de chamados e gestão de ativos.

4.51.6. PAMs (CyberArk, BeyondTrust, Thycotic, Centrify ou equivalentes).

4.51.7. Provedores de nuvem (AWS, Azure, GCP) e diretórios (LDAP/Active Directory).

4.52. d) Compatibilidade e Suporte a Ambientes

4.52.1. A solução deverá realizar varreduras em sistemas operacionais Windows, Linux, macOS, Unix (Solaris, AIX, IBM) e *appliances virtuais*.

4.52.2. Deve suportar ambientes híbridos, contemplando *on-premises*, nuvem pública, nuvem privada e aplicações SaaS.

4.52.3. Deve suportar dispositivos IoT, SCADA/OT, mobile *devices* e *aplicações web*.

4.53. e) Desempenho e Escalabilidade

4.53.1. A solução deve permitir orquestração ilimitada de *scanners* dentro da infraestrutura do Contratante.

4.53.2. Deve possibilitar varreduras distribuídas por múltiplas localidades e nuvens.

4.53.3. Deverá permitir agendamento automático de varreduras e geração de relatórios customizados.

4.53.4. O processamento deve garantir baixa interferência na rede e otimização de tráfego durante escaneamentos.

4.54. f) Armazenamento e Banco de Dados

4.54.1. A solução deve dispor de modelo de armazenamento integrado que não dependa de banco de dados externo.

4.54.2. Caso haja dependência de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela contratada.

4.54.3. Todos os resultados de varreduras e informações correlacionadas deverão ser criptografados em trânsito e em repouso.

4.55. g) Interfaces de Gerenciamento

4.55.1. A console de gerenciamento deverá suportar acesso simultâneo para no mínimo 10 usuários.

4.55.2. Deve disponibilizar *dashboards* customizáveis, relatórios em múltiplos formatos (HTML, PDF, CSV) e trilhas de auditoria.

4.55.3. A interface deve ser acessível via navegador web, com suporte a MFA e SSO.

4.56. **Requisitos de Projeto e de Implementação**

4.57. a) Planejamento da Implementação

4.57.1. A contratada deverá elaborar um plano de instalação detalhado, incluindo fases, cronograma, requisitos prévios, responsáveis e marcos de entrega.

4.57.2. O plano deverá ser submetido à aprovação do Contratante antes do início da execução.

4.58. b) Instalação e Configuração

4.58.1. A contratada será responsável por instalar todos os componentes da solução (console, sensores, agentes, integrações).

4.58.2. Deverá configurar:

4.58.3. Perfis de varredura (credenciada e não credenciada).

4.58.4. Perfis de usuários (RBAC).

4.58.5. Políticas de agendamento e janelas de escaneamento.

4.58.6. Integração com Active Directory, LDAP, nuvens públicas (AWS, Azure, GCP) e SIEMs.

4.58.7. Todas as configurações devem estar alinhadas com as boas práticas do fabricante.

4.59. c) Testes de Aceitação e Homologação

4.59.1. A contratada deverá executar testes de validação em pelo menos 3 varreduras distintas, contemplando:

4.59.2. Cobertura de ativos.

4.59.3. Detecção de vulnerabilidades conhecidas.

4.59.4. Avaliação de falsos positivos.

4.59.5. Impacto de rede e desempenho do scanner.

4.59.6. Serão realizados testes de homologação do projeto, verificando estabilidade da solução e consistência das descobertas.

4.60. d) Documentação Técnica

4.60.1. A contratada deverá entregar um relatório *as-built*, incluindo:

4.60.2. Arquitetura lógica e física implantada.

4.60.3. Configurações aplicadas.

4.60.4. Perfis de varredura criados.

4.60.5. Procedimentos operacionais padrão (POPs).

4.60.6. Plano de continuidade e recomendações de boas práticas.

4.61. e) Critérios de Aceite

4.61.1. Execução satisfatória dos testes de aceitação e homologação.

4.61.2. Disponibilidade da console centralizada com *dashboards* e relatórios operacionais.

4.61.3. Entrega da documentação técnica completa e validada.

4.61.4. Treinamento ministrado para a equipe do Contratante antes da liberação para produção.

4.62. f) Entregáveis do Projeto

4.62.1. Plano de instalação aprovado.

4.62.2. Relatórios de validação e homologação.

4.62.3. Relatório técnico *as-built*.

4.62.4. Perfis de varredura, políticas e integrações configurados.

4.62.5. Documentação final consolidada.

4.63. **Requisitos de Implantação**

4.64. a) Responsabilidades da Contratada

4.64.1. Executar a instalação completa da solução contratada, abrangendo todos os componentes (console de gerenciamento, scanners, sensores e agentes).

4.64.2. Apoiar o Contratante na definição da arquitetura de implantação, incluindo topologia, pontos de análise e regras iniciais de gestão de vulnerabilidades.

4.64.3. Aplicar todas as licenças e patches de atualização necessários ao funcionamento pleno da solução.

4.64.4. Configurar usuários administradores, perfis de acesso e serviços essenciais de rede.

4.65. b) Procedimentos de Implantação

4.65.1. Implantar a solução de acordo com as boas práticas do fabricante e normas de segurança aplicáveis.

4.65.2. Realizar mínimo de três varreduras iniciais para validação da operação em diferentes contextos (ativos de rede, aplicações, nuvem).

4.65.3. Efetuar testes de validação e homologação, assegurando estabilidade, cobertura de ativos e precisão na detecção de vulnerabilidades.

4.65.4. Emitir relatório de aceitação técnica comprovando o funcionamento da solução em ambiente produtivo.

4.66. c) Integrações Obrigatórias na Implantação

4.66.1. Integração com Active Directory/LDAP para varreduras autenticadas.

4.66.2. Integração com nuvens públicas (AWS, Azure, GCP) para avaliação de workloads e instâncias.

4.66.3. Integração com SIEM e ITSM para correlação de eventos e abertura de chamados.

4.66.4. Integração com ferramentas de gerenciamento de acessos privilegiados (PAMs).

4.67. d) Documentação de Implantação

4.67.1. Entregar relatório *as-built* da implantação contendo:

4.67.2. Diagramas lógicos e físicos (quando aplicável).

4.67.3. Perfis de varredura e políticas de risco configurados.

4.67.4. Registro de integrações realizadas.

4.67.5. Procedimentos operacionais e recomendações de uso seguro.

4.68. e) Critérios de Aceitação da Implantação

4.68.1. Confirmação de que a solução está operacional e atende ao escopo contratado.

4.68.2. Execução bem-sucedida dos testes de varredura e homologação.

4.68.3. Entrega de documentação técnica e relatório *as-built*.

4.68.4. Liberação formal para operação pela equipe do Contratante.

4.69. **Requisitos de Garantia e Manutenção**

4.70. a) Garantia das Licenças

4.70.1. Todas as licenças fornecidas (Itens 1, 2, 3 e 4) deverão possuir garantia oficial do fabricante pelo período de 36 (trinta e seis) meses, assegurando pleno funcionamento e acesso a novas versões e atualizações.

4.70.2. As licenças deverão estar registradas em nome do Contratante, sendo vedada a utilização de licenças de terceiros ou prestadores de serviços.

4.71. b) Garantia da Solução

4.71.1. Durante o período de vigência contratual, a contratada deverá garantir:

4.71.2. Disponibilidade contínua da solução.

4.71.3. Aplicação de *patches* de segurança e correções de bugs.

4.71.4. Acesso às novas funcionalidades lançadas pelo fabricante, sem custos adicionais.

4.71.5. Qualquer falha identificada deverá ser corrigida pela contratada dentro dos prazos acordados em SLA.

4.72. c) Manutenção Evolutiva, Corretiva e Preventiva

4.72.1. O serviço continuado (Item 7) deverá contemplar:

4.72.2. Manutenção preventiva: aplicação de atualizações, ajustes de configuração e acompanhamento de desempenho.

4.72.3. Manutenção corretiva: solução de falhas e incidentes identificados.

4.72.4. Manutenção evolutiva: ajustes decorrentes de novas versões ou funcionalidades liberadas pelo fabricante.

4.72.5. Todas as manutenções deverão ser registradas em relatórios técnicos contendo data, hora, responsável e resultado da ação.

4.73. d) Atendimento e Suporte Técnico

4.73.1. O atendimento deverá ser prestado na modalidade 24x7x365, com prazo máximo de 2 horas para resposta após a abertura de solicitação.

4.73.2. O suporte poderá ser remoto ou presencial (quando solicitado pelo Contratante).

4.73.3. O atendimento deverá ser realizado por profissionais certificados na solução contratada.

4.74. e) Relatórios e Indicadores de Garantia

4.74.1. A contratada deverá entregar relatórios semestrais (ou sob demanda) sobre panorama de vulnerabilidades, ações de remediação, incidentes tratados e evolução do risco.

4.74.2. Indicadores mínimos:

4.74.3. % de ativos críticos cobertos por varreduras recentes.

4.74.4. Tendência de vulnerabilidades abertas/fechadas.

4.74.5. MTTR (tempo médio de resolução).

4.74.6. Conformidade com SLAs.

4.75. f) Continuidade Operacional

4.75.1. A contratada deverá assegurar a continuidade do serviço, mesmo em casos de atualizações críticas, mudanças de versão ou substituição de componentes da arquitetura.

4.75.2. A solução deverá manter compatibilidade com integrações existentes (SIEM, ITSM, AD, nuvens) ao longo da vigência do contrato.

4.76. **Requisitos de Experiência Profissional**

4.77. a) Experiência da Contratada

4.77.1. A empresa contratada deverá comprovar experiência prévia em implantação, suporte e manutenção de soluções de gestão de vulnerabilidades de porte e complexidade semelhantes às do Contratante.

4.77.2. Será exigida comprovação documental de pelo menos 1 (um) contrato anterior com administração pública ou instituição privada de grande porte, em que tenha realizado serviços equivalentes aos itens do objeto (instalação, suporte continuado e treinamento).

4.77.3. Para remover a subjetividade da análise o(s) atestado(s) de capacidade técnica deverá(ão) comprovar que a licitante possui experiência prévia na solução ofertada, englobando no mínimo, 50% da volumetria e complexidade técnica de 2 (dois) tipos distintos de licenças descritas neste Termo de Referência.

4.78. b) Experiência em Treinamento

4.78.1. O instrutor responsável pelo treinamento deverá possuir experiência comprovada na condução de capacitações técnicas em soluções de segurança da informação.

4.78.2. Preferencialmente, deverá ter atuado em pelo menos 2 treinamentos prévios ministrados sobre ferramentas de gestão de vulnerabilidades.

4.79. **Requisitos de Formação da Equipe**

4.80. a) Formação Acadêmica

4.80.1. Os profissionais alocados para os serviços de instalação, suporte e treinamento deverão possuir formação de nível superior em cursos relacionados à área de Tecnologia da Informação, tais como: Ciência da Computação, Engenharia da Computação, Sistemas de Informação, Redes de Computadores ou equivalentes.

4.80.2. Alternativamente, poderá ser aceita formação de nível médio/técnico em informática ou redes, desde que acompanhada de experiência prática comprovada em segurança da informação e administração de sistemas.

4.81. b) Certificações Técnicas

4.81.1. Pelo menos um profissional da equipe deverá possuir certificação reconhecida em gestão de vulnerabilidades ou segurança da informação.

4.81.2. Para o instrutor de treinamento, será obrigatória certificação técnica na ferramenta contratada, emitida ou reconhecida pelo fabricante.

4.82. c) Composição da Equipe da Contratada

4.82.1. Engenheiro de implantação: responsável pela instalação, integração e configuração da solução.

4.82.2. Analista de suporte: responsável pelo atendimento 24x7, aplicação de patches, acompanhamento de incidentes e geração de relatórios.

4.82.3. Instrutor de treinamento: profissional certificado para capacitar a equipe do Contratante no uso da solução.

4.83. d) Equipe Mínima Exigida

4.83.1. A contratada deverá garantir que, durante todo o contrato, haja disponibilidade mínima de:

4.83.2. 1 (um) engenheiro certificado para implantação e integrações.

4.83.3. 1 (um) analista certificado para suporte técnico contínuo.

4.83.4. 1 (um) instrutor certificado para treinamento por plataforma.

4.84. **Requisitos de Metodologia de Trabalho**

4.85. a) Metodologia de Execução

4.85.1. A contratada deverá adotar metodologia estruturada, baseada em boas práticas de gestão de projetos (ex.: PMBOK, PRINCE2 ou equivalente), contemplando:

4.85.2. Levantamento inicial do ambiente e requisitos.

4.85.3. Elaboração de plano de instalação com fases, responsáveis e cronograma.

4.85.4. Execução da implantação conforme boas práticas do fabricante.

4.85.5. Testes de aceitação e homologação.

4.85.6. Entrega do relatório *as-built* e documentação técnica.

4.86. b) Metodologia de Operação

4.86.1. O serviço continuado deverá ser executado com base em processos de ITIL ou equivalentes, incluindo:

4.86.2. Gerenciamento de incidentes.

4.86.3. Gerenciamento de mudanças.

4.86.4. Gerenciamento de problemas.

4.86.5. Geração de relatórios e indicadores.

4.86.6. As atividades deverão contemplar acompanhamento proativo, suporte reativo e evolução contínua

da solução.

4.87. c) Metodologia de Treinamento

4.87.1. O treinamento deverá ser ministrado de forma remota, síncrona e interativa, priorizando abordagem prática (*hands-on*).

4.87.2. Cada sessão deverá conter:

4.87.3. Apresentação conceitual.

4.87.4. Demonstrações práticas na solução implantada.

4.87.5. Exercícios simulados.

4.87.6. Avaliação final de aprendizado.

4.87.7. O conteúdo deverá ser padronizado e acompanhado de material didático digital (apostila ou guia de referência).

4.88. d). Metodologia de Relatórios e Entregáveis

4.88.1. Relatórios técnicos e gerenciais deverão seguir formato padronizado, contendo: panorama de vulnerabilidades, indicadores de risco, recomendações de remediação e tendências históricas.

4.88.2. Relatórios semestrais do serviço continuado deverão consolidar evolução, métricas e recomendações estratégicas.

4.89. e). Metodologia de Comunicação com o Contratante

4.89.1. A contratada deverá estabelecer canal de comunicação dedicado para abertura de chamados e acompanhamento de demandas.

4.89.2. O fluxo de comunicação deverá contemplar níveis de escalonamento e prazos por criticidade, alinhados ao SLA.

4.89.3. Reuniões de acompanhamento poderão ser realizadas periodicamente para alinhamento técnico e estratégico.

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

4.91. a) Conformidade Normativa e Legal

4.91.1. A solução deverá estar aderente à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), assegurando que o tratamento das informações seja feito exclusivamente para a finalidade contratual.

4.91.2. Para soluções em nuvem (SaaS), deverá ser atendido o disposto no Art. 18 da IN SGD/ME nº 05/2021, garantindo que os dados e *metadados* do Contratante estejam hospedados em território nacional, com pelo menos uma cópia de segurança no Brasil.

4.91.3. A solução deverá estar em conformidade com normas e boas práticas reconhecidas, como ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework e CIS Benchmarks.

4.92. b) Criptografia e Proteção dos Dados

4.92.1. Todos os dados de varredura, relatórios, evidências e credenciais deverão ser criptografados em trânsito e em repouso.

4.92.2. A solução deve permitir o armazenamento seguro de credenciais utilizadas em varreduras autenticadas (LDAP, Active Directory, root em Linux etc.).

4.92.3. Deverá ser garantida a integridade e confidencialidade das informações processadas, com proteção contra manipulação indevida ou acesso não autorizado.

4.93. c) Controle de Acesso e Autenticação

4.93.1. Implementação obrigatória de controle de acesso baseado em perfis (RBAC), permitindo restrição de funcionalidades e relatórios por grupo de usuários.

4.93.2. Suporte a autenticação via MFA (Multi-Factor Authentication) e SAML/SSO para integração com diretórios corporativos.

4.93.3. Registro e rastreabilidade completa das ações dos usuários por meio de trilhas de auditoria exportáveis.

4.94. d) Gestão de Incidentes e Continuidade

4.94.1. A contratada deverá notificar imediatamente o Contratante em caso de incidente de segurança que envolva os dados ou serviços contratados.

4.94.2. A solução deverá contemplar mecanismos de alta disponibilidade, redundância e plano de

continuidade.

4.94.3. Deverá existir funcionalidade de reversibilidade e portabilidade, permitindo exportação integral dos dados e históricos em formato aberto (CSV, JSON, PDF).

4.95. e) Segurança Operacional

4.95.1. A solução deverá permitir a exclusão de determinados ativos ou IPs do escopo de varredura, conforme políticas internas do Contratante.

4.95.2. Os resultados das varreduras deverão incluir evidências técnicas (outputs) que comprovem a vulnerabilidade encontrada.

4.95.3. A solução deverá garantir atualização contínua do banco de vulnerabilidades a partir de múltiplas fontes (NVD, GitHub, *advisories* de fabricantes, CISA etc.).

4.96. f) Responsabilidade da Contratada

4.96.1. A contratada deverá assinar termo de confidencialidade, assegurando que nenhum dado do Contratante será compartilhado ou transferido sem autorização formal.

4.96.2. O serviço continuado deverá incluir monitoramento constante da exposição cibernética, com emissão de alertas em tempo real para vulnerabilidades críticas.

4.96.3. A contratada deverá emitir relatórios periódicos de segurança (mínimo semestrais) contendo panorama de vulnerabilidades, incidentes reportados e medidas de mitigação adotadas.

4.97. **Requisito de Sustentabilidade**

4.98. a) Sustentabilidade Ambiental

4.98.1. Sempre que possível, a solução deverá ser fornecida em modelo *SaaS* ou hospedada em nuvem, priorizando data centers energeticamente eficientes, com uso de energia renovável e iniciativas de neutralização de carbono.

4.98.2. A contratada deverá adotar práticas que reduzam o impacto ambiental, incluindo a diminuição do consumo de papel, privilegiando relatórios e registros em formato digital (HTML, PDF, CSV).

4.98.3. Recomenda-se que a contratada apresente certificações ambientais (ex.: ISO 14001 ou equivalentes), ou evidências de políticas corporativas voltadas para sustentabilidade ambiental.

4.99. b) Sustentabilidade Social e de Governança (ESG)

4.99.1. A contratada deverá observar princípios de ética, integridade e responsabilidade social, promovendo boas práticas de governança em alinhamento com a Lei Anticorrupção (Lei nº 12.846/2013).

4.99.2. Deverá garantir a promoção de uma cultura organizacional de segurança da informação, que fortaleça a cidadania digital e a conscientização dos usuários internos do Contratante.

4.99.3. A empresa deverá respeitar normas de diversidade, inclusão e acessibilidade, assegurando condições justas e seguras para seus colaboradores.

4.100. c) Sustentabilidade Econômica e Tecnológica

4.100.1. A solução deve ser projetada para uso eficiente de recursos computacionais, com escalabilidade sob demanda, evitando desperdícios de capacidade de processamento, armazenamento e licenciamento.

4.100.2. O contrato deve garantir a evolução contínua da solução, sem necessidade de substituição precoce ou aquisições adicionais que aumentem a pegada ambiental.

4.100.3. A contratada deverá assegurar a portabilidade e reversibilidade da solução, evitando dependência tecnológica que comprometa a sustentabilidade do investimento público.

4.101. d) Compromisso com a Continuidade Sustentável

4.101.1. Relatórios periódicos da contratada deverão incluir recomendações para otimização de recursos e redução de impactos ambientais relacionados à operação da solução.

4.101.2. O Contratante poderá solicitar à contratada comprovação de práticas sustentáveis nos data centers, operações de suporte e logística envolvidas na prestação do serviço.

4.102. **VISTORIA**

4.102.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

4.103. **SUBCONTRATAÇÃO**

4.103.1. É admitida a subcontratação parcial do objeto, nas seguintes condições:

4.103.1.1. A subcontratação fica **limitada** a prestação dos serviços de implantação e capacitação previstos no objeto. Sob nenhuma hipótese, a subcontratação exime a CONTRATADA de suas responsabilidades legais com

a CONTRATANTE, sendo ela a entidade associada as sanções administrativas cabíveis do processo.

4.103.2. É vedada a subcontratação no fornecimento dos licenciamentos previstos no objeto.

4.104. **CONSÓRCIO**

4.104.1. Avaliou-se a viabilidade de participação de empresas em consórcio na presente contratação. Concluiu-se, contudo, que a formação de consórcios não se mostra adequada nem vantajosa, em razão da natureza integrada do objeto, que envolve licenciamento de solução tecnológica, serviços especializados de implantação, capacitação e suporte contínuo, demandando responsabilização técnica e contratual centralizada.

4.104.2. A admissão de consórcios poderia acarretar fragmentação de responsabilidades, maior complexidade na fiscalização contratual e riscos à continuidade e à qualidade da execução, sem que se identifique ganho efetivo de competitividade ou economicidade para a Administração.

4.105. **DA VERIFICAÇÃO DE AMOSTRA DO OBJETO**

4.106. Não será exigida amostra. Porém, será exigida c omprovação técnica individualizada por item proposto. Cada item ofertado deverá estar acompanhado de documentação técnica (tais como catálogos, manuais, fichas técnicas ou declarações do fabricante), que comprove, de forma clara e objetiva, o atendimento a todos os requisitos estabelecidos nas especificações técnicas correspondentes. Tal verificação será exigida durante a **qualificação técnica da licitação**.

4.107. **GARANTIA DA CONTRATAÇÃO**

4.107.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, podendo o Contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a 5% (cinco por cento) do valor anual da contratação.

4.107.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.107.3. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.

4.107.4. Caso o adjudicatário não apresente a apólice de seguro-garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

4.107.5. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal, mediante a emissão do respectivo endosso pela seguradora.

4.107.6. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e que nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

4.107.7. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro, títulos da dívida pública, fiança bancária ou título de capitalização.

4.107.8. Caso seja a garantia em dinheiro a modalidade escolhida pelo Contratado, esta deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

4.107.9. Caso a opção seja pela utilização de títulos da dívida pública, estes deverão 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 competente.

4.107.10. No caso de garantia na modalidade de fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, contendo expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

4.107.11. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedade de capitalização regularmente constituída e autorizada pelo Governo Federal.

4.107.12. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela SUSEP, nos termos do art. 8º, inciso III, da Circular SUSEP nº 656, de 11 de março de 2022.

4.107.13. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

4.107.13.1. prejuízos advindos do não cumprimento do objeto do contrato e do inadimplemento das demais obrigações nele previstas;

4.107.13.2. multas moratórias e punitivas aplicadas pela Administração à contratada; e

4.107.13.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, quando decorrentes da execução contratual, não adimplidas pelo Contratado.

4.107.14. Em caso de seguro-garantia, a apólice deverá prever cobertura para pagamento direto ao empregado, após decisão definitiva em processo administrativo que apure montante líquido e certo a ele devido em razão de inadimplemento do Contratado, independentemente de trânsito em julgado de decisão judicial.

4.107.15. No caso de alteração do valor do contrato ou de prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, observados os mesmos parâmetros utilizados quando da contratação.

4.107.16. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.107.17. Se o valor da garantia for utilizado, total ou parcialmente, em pagamento de qualquer obrigação, o Contratado obriga-se a promover a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da data em que for formalmente notificado.

4.107.18. O Contratante executará a garantia na forma prevista na legislação aplicável.

4.107.19. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.107.20. No caso de seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora dessa vigência, não caracterizando motivo para negativa de cobertura, desde que respeitados os prazos prescricionais aplicáveis ao contrato de seguro, nos termos do art. 20 da Circular SUSEP nº 662, de 11 de abril de 2022.

4.107.21. Extinguir-se-á a garantia com a restituição da carta fiança, a autorização para liberação de valores depositados em dinheiro a título de garantia ou a anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu integralmente as cláusulas contratuais.

4.107.22. A extinção da garantia na modalidade seguro-garantia observará a regulamentação específica da SUSEP.

4.107.23. A Administração deverá apurar a existência de pendências contratuais antes do término da vigência da apólice.

4.107.24. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após sua extinção por culpa exclusiva da Administração e, quando prestada em dinheiro, será atualizada monetariamente.

4.107.25. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.107.26. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

4.107.27. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

5. DOS QUANTITATIVOS ESTIMADOS E DOS ÓRGÃOS PARTICIPANTES DA INTENÇÃO DE REGISTRO DE PREÇOS

5.1. **Considerações Gerais:**

5.1.1. Os quantitativos estimados da presente contratação foram definidos a partir da Intenção de Registro de Preços regularmente instaurada, considerando as manifestações formais de interesse apresentadas pelos órgãos participantes, bem como a necessidade estimada do órgão gerenciador, nos termos do Decreto nº 11.462, de 31 de março de 2023.

5.1.2. Os órgãos participantes encaminharam suas estimativas de consumo com base em planejamento interno próprio, sendo tais informações consolidadas pela Administração para fins de dimensionamento da licitação e formação da Ata de Registro de Preços.

5.1.3. Ressalta-se que os quantitativos indicados possuem natureza estimativa, não constituindo obrigação de contratação integral por parte da Administração, nos termos do art. 83 da Lei nº 14.133, de 2021.

5.2. **Órgão gerenciador:**

5.2.1. Atua como órgão gerenciador da presente Ata de Registro de Preços o:

5.2.2. **Conselho Federal de Engenharia e Agronomia – CONFEA**

5.2.3. O quantitativo estimado do órgão gerenciador encontra-se detalhado na planilha consolidada que integra o presente Termo de Referência.

5.3. **Órgãos participantes da Intenção de Registro de Preços**

5.3.1. Manifestaram formalmente interesse em participar da presente Intenção de Registro de Preços, conforme documentos anexos ao processo administrativo, os seguintes órgãos:

5.3.2. Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome – MDS

5.3.3. Secretaria de Estado da Educação de Rondônia – SEDUC/RO

5.3.4. Instituto de Desenvolvimento Florestal e da Biodiversidade do Estado do Pará – IDEFLOR-Bio/PA

5.3.5. Os quantitativos estimados por cada órgão participante foram informados individualmente, conforme suas respectivas manifestações de interesse, e encontram-se consolidados na planilha de quantitativos e preços que integra este Termo de Referência.

5.4. **Consolidação dos quantitativos**

5.4.1. Os quantitativos totais da contratação correspondem à soma das estimativas apresentadas pelo órgão gerenciador e pelos órgãos participantes, estando organizados de forma consolidada, por item, na planilha intitulada:

5.4.2. “Planilha de Quantitativos e Pesquisa de Preços – ETP / Registro de Preços”

5.4.3. referida planilha constitui parte integrante e indissociável deste Termo de Referência, servindo de base para:

a) definição do valor estimado da contratação;

b) julgamento das propostas;

c) futura formalização das contratações decorrentes da Ata de Registro de Preços.

5.5. **Vinculação à Ata de Registro de Preços**

5.5.1. Os quantitativos estimados aqui descritos servirão exclusivamente para fins de registro de preços, não implicando direito subjetivo à contratação, nem obrigação da Administração de contratar qualquer quantitativo mínimo, podendo os órgãos aderentes realizar contratações conforme suas necessidades, durante a vigência da Ata.

6. PAPÉIS E RESPONSABILIDADES

6.1. **SÃO OBRIGAÇÕES DA CONTRATANTE**

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

6.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

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

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

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

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

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

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

6.2. **SÃO OBRIGAÇÕES DO CONTRATADO**

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

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

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

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

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

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

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

6.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

6.2.9. fazer a transição contratual, quando for o caso;

6.3. **SÃO OBRIGAÇÕES DO ÓRGÃO GERENCIADOR DO REGISTRO DE PREÇOS:**

6.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

6.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

6.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

6.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

6.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

6.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

6.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

6.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

6.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. **CONDIÇÕES DE EXECUÇÃO:**

7.2. A execução do objeto seguirá a seguinte dinâmica:

7.2.1. Início da execução do objeto: até 15 (quinze) dias úteis da assinatura do contrato OU da emissão da Ordem de Serviço, o que ocorrer por último.

7.2.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias, procedimentos, frequência e periodicidade de execução do trabalho:

7.2.3. Instalação e configuração da solução de Gestão de Vulnerabilidades, contemplando os módulos de ativos, aplicações web, superfície de ataque e Active Directory;

7.2.4. Realização de no mínimo 3 varreduras iniciais de validação (ativos internos, externos e *aplicações web*);

7.2.5. Homologação conjunta com a equipe técnica do Contratante, mediante relatório de aceitação (*as-built*);

7.2.6. Capacitação da equipe técnica em até 30 dias após a instalação, com carga horária mínima de 16h por solução;

7.2.7. Execução de varreduras contínuas e periódicas (mensais para ativos internos, semanais para aplicações web e diárias para ativos críticos expostos);

7.2.8. Prestação do serviço continuado de monitoramento e suporte 24x7, com relatórios semestrais e reuniões de acompanhamento.

7.3. **Cronograma de realização dos serviços:**

7.3.1. Etapa 1 – Planejamento da implantação: até 10 dias após a assinatura.

7.3.2. Etapa 2 – Instalação e configuração: até 30 dias após o início da execução.

7.3.3. Etapa 3 – Testes de aceitação e homologação: até 45 dias após o início da execução.

7.3.4. Etapa 4 – Treinamento da equipe técnica: até 60 dias após o início da execução.

7.3.5. Etapa 5 – Serviço continuado de gestão de vulnerabilidades: durante os 36 meses de vigência contratual.

7.4. **Local e horário da prestação dos serviços**

7.4.1. Para o CONFEA:

7.4.1.1. Os serviços serão prestados nas dependências do Confea (SEPN 508 – Bloco A – Brasília/DF), podendo ocorrer de forma remota ou híbrida conforme necessidade operacional.

7.4.1.2. Horário de atendimento técnico remoto: 24x7x365.

7.4.1.3. Atendimento presencial, quando demandado, em dias úteis, das 9h às 18h.

7.4.1.4. Para os outros órgãos que participaram da IRP:

7.4.2. Deverá ser verificado no ato da assinatura do contrato.

7.5. **Materiais a serem disponibilizados**

7.5.1. A contratada deverá disponibilizar:

7.5.2. Licenças de *software* originais e em nome do Confea, com validade de 36 meses;

7.5.3. Acesso à console de gerenciamento e aos módulos contratados;

7.5.4. Recursos de infraestrutura necessários para hospedagem SaaS, quando aplicável;

7.5.5. Documentação técnica, manuais de operação, relatórios e materiais de treinamento.

7.6. **Informações relevantes para o dimensionamento da proposta**

7.6.1. A demanda do órgão tem como base as seguintes características:

7.6.2. Parque tecnológico com mais de 700 ativos entre servidores, estações, *appliances* e aplicações *web*;

7.6.3. Crescimento projetado do ambiente de TI em torno de 10% ao ano;

7.6.4. Necessidade de gestão contínua de vulnerabilidades, com integração a Active Directory, nuvens públicas e SIEM;

7.6.5. Atendimento aos normativos de LGPD, E-Ciber, ISO 27001/27002 e IN SGD/ME nº 94/2022.

7.7. **Especificação da garantia do serviço**

7.7.1. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente ao recebimento definitivo do objeto.

7.8. **Formas de transferência de conhecimento**

7.8.1. Treinamento remoto e síncrono, com carga mínima de 16h por solução contratada;

7.8.2. Entrega de material didático (slides, guias e gravações, quando possível);

7.8.3. Sessões práticas durante a instalação e configuração, assegurando a autonomia da equipe técnica do Confea.

7.9. **Procedimentos de transição e finalização do contrato**

7.9.1. Entrega de relatório técnico as-built com arquitetura, configurações e integrações realizadas;

7.9.2. Transferência integral de dados, históricos e relatórios em formatos abertos (CSV, JSON, PDF);

7.9.3. Encerramento formal com reunião de transição, orientando sobre continuidade ou eventual substituição da solução.

7.10. **Quantidade mínima de serviços para comparação e controle**

7.10.1. Cada Ordem de Serviço conterá o volume de licenças ou atividades demandadas, o prazo de execução e a localização (remoto ou presencial), conforme modelo descrito em anexo ao contrato.

7.11. **Mecanismos formais de comunicação**

7.11.1. Ordem de Serviço (OS);

7.11.2. Ata de Reunião;

7.11.3. Ofício;

7.11.4. Sistema de abertura de chamados;

7.11.5. E-mails e correspondências oficiais;

7.11.6. Reuniões de acompanhamento técnico e gerencial periódicas.

7.12. **MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA**

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

7.14. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos documento Anexos.

8. MODELO DE GESTÃO DO CONTRATO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

8.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

8.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

8.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

8.5. **PREPOSTO**

8.5.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

8.5.2. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

8.6. **REUNIÃO INICIAL**

8.7. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

8.8. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até (10) dias úteis da assinatura do Contrato, poden do ser prorrogada a critério da Contratante.

8.8.1. A pauta desta reunião observará, pelo menos:

8.8.1.1. Presença do representante legal da contratada, que apresentará o seu preposto;

8.8.1.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

8.8.1.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

8.8.1.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

8.8.1.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

8.9. **FISCALIZAÇÃO**

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

8.11. **FISCALIZAÇAO TECNICA**

8.12. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

8.12.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);[MM2]

8.12.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

8.12.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

8.12.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

8.12.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

8.13. **FISCALIZAÇÃO ADMINISTRATIVA**

8.14. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

8.14.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

8.15. **GESTOR DO CONTRATO**

8.15.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

8.15.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

8.15.3. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

8.15.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

8.15.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

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

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

nos termos do contrato.

9. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

9.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme disposto neste item.

IAP – ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	***Descrição***
Finalidade	*Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Serviço.*
Meta a cumprir	*IAP igual ou superior a (95)%.*
Instrumento de medição	*Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.*
Forma de acompanhamento	*É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência.*
Periodicidade	*Mensal*
Mecanismo de Cálculo (métrica)	***IAP = 100 * (ΣQtap / ΣQtr)*** *Onde:* *IAP = Indicador de atendimento aos prazos do serviço;* *ΣQtap = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência;* *ΣQtr = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.*
Observações	*Obs1: Serão utilizados dias corridos na medição.* *Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.*
Início de Vigência	*A partir da emissão da OS.*
Faixas de ajuste no pagamento e Sanções	*IAP >= 90%: sem descontos sobre o valor da fatura mensal.* *IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.* *IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal.* *IAP < 70%: 30% de desconto sobre o valor da fatura mensal.*

9.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

9.1.2. não produzir os resultados acordados;

9.1.3. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

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

9.2. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

9.3. **A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:**

9.3.1. a) Cumprimento dos prazos e níveis de serviço estabelecidos, medidos por meio do Índice de Atendimento no Prazo (IAP), conforme metodologia descrita neste Termo de Referência, observando-se as faixas de desempenho e respectivas glosas automáticas;

9.3.2. b) Entrega e aceite dos relatórios técnicos mensais e semestrais, contendo o histórico de varreduras, vulnerabilidades identificadas, recomendações de mitigação e evidências das ações executadas;

9.3.3. c) Manutenção da disponibilidade operacional da solução igual ou superior a 99,5%, considerando o período de medição mensal;

9.3.4. d) Atendimento aos Acordos de Nível de Serviço (SLA), com tempo médio de resposta (MTTA) de até 2 horas e tempo médio de resolução (MTTR) de até 8 horas para incidentes críticos;

9.3.5. e) Correção das vulnerabilidades classificadas como críticas ou altas dentro dos prazos definidos neste Termo de Referência ou nos planos de ação acordados com a fiscalização;

9.3.6. f) Participação nas reuniões de acompanhamento técnico, sempre que convocada pela fiscalização, para apresentação dos resultados, ajustes de cronograma e evolução das ações corretivas;

9.3.7. g) Entrega do relatório final de desempenho, consolidando as métricas de operação, disponibilidade, atendimento e evolução da postura de segurança durante a vigência contratual, devidamente aceito pela fiscalização.

9.3.8. Condição de pagamento:

9.3.9. O pagamento das parcelas mensais estará condicionado ao aceite formal da fiscalização, com base nos relatórios técnicos e evidências de cumprimento das metas estabelecidas neste instrumento.

9.3.10. **DO RECEBIMENTO**

9.4. Os serviços serão recebidos provisoriamente, no prazo de 5 (cinco) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

9.4.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

9.5. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

9.6. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

9.7. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

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

9.8.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

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

9.10. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

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

9.12. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.13. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.14. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.14.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

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

9.14.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.14.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado

pela fiscalização.

9.14.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

9.15. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.16. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

9.17. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9.18. **SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO**

9.19. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	***Ocorrência***	***Glosa / Sanção***
1	*Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (24) horas úteis.*	*Multa de (0,1) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de (5) dias úteis.*
		Após o limite de (5) dias úteis, aplicar-se-á multa de (2) % do valor total do Contrato.
2	*Não atender ao indicador de nível de serviço IAP (Índice de Atendimento no Prazo)*	*IAP >= 90%: sem descontos sobre o valor da fatura mensal.*
		IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.
		IAP >= 70% e < 80%: 20% de desconto sobre o valor da fatura mensal.
		IAP < 70%: 30% de desconto sobre o valor da fatura mensal.
3	*Não cumprir qualquer outra obrigação contratual não citada nesta tabela.*	*Advertência.* *Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de (2) % do valor total do Contrato.*

tabela 1.1

Tabela de Ocorrências, Sanções e Glosas

Nº	**Ocorrência / Falha Identificada**	**Prazo para Correção / Esclarecimento**	**Glosa / Sanção Aplicável**	**Observações / Critério de Aplicação**
1	Não prestar os esclarecimentos imediatamente, referentes à execução dos serviços, salvo quando implicarem em indagações de caráter técnico.	24 horas úteis	Multa de **0,1%** sobre o valor total do Contrato por dia útil de atraso, até o limite de **5 dias úteis**. Após esse prazo, multa de **2%** sobre o valor total do Contrato.	Incide sobre a ausência de resposta a solicitações formais da fiscalização.
2	Atraso na entrega de produtos, relatórios ou etapas previstas no cronograma contratual.	Conforme cronograma aprovado	Multa de mora de **0,2%** ao dia sobre o valor da etapa ou parcela atrasada, limitada a **10%** do valor total do Contrato.	Aplicável cumulativamente à glosa proporcional quando houver prejuízo direto.

Nº	Ocorrência / Falha Identificada	Prazo para Correção / Esclarecimento	Glosa / Sanção Aplicável	Observações / Critério de Aplicação
3	Execução de serviços em desconformidade com as especificações técnicas do Termo de Referência ou da Ordem de Serviço.	3 dias úteis após notificação	Glosa proporcional ao percentual de não conformidade; persistindo a falha, multa de **1%** sobre o valor total do Contrato.	Avaliação técnica da fiscalização.
4	Ausência ou substituição de profissional sem prévia anuência da Contratante.	Imediato	Multa de **0,5%** do valor mensal do contrato por ocorrência.	Não afasta a obrigação de recompor a equipe.
5	Falta de comparecimento a reuniões convocadas pela fiscalização.	1 dia útil	Multa de **0,1%** do valor mensal do contrato por ocorrência.	Considera-se reunião previamente convocada com antecedência mínima de 24h.
6	Descumprimento dos prazos de correção de não conformidades apontadas em relatório de acompanhamento.	Conforme prazo fixado em relatório	Multa de **0,2%** do valor mensal do contrato por dia útil de atraso, limitada a **10%** do valor mensal.	O não atendimento poderá ensejar retenção no pagamento.
7	Não disponibilizar relatórios, indicadores ou evidências exigidas para aferição dos níveis de serviço (SLA).	2 dias úteis	Glosa proporcional de **até 10%** do valor mensal do contrato, conforme gravidade.	Base para retenção até regularização.
8	Inobservância dos prazos de comunicação de indisponibilidade, incidentes ou falhas críticas.	Imediato	Multa de **0,1%** por hora de atraso na comunicação, limitada a **5%** do valor mensal.	Considera-se comunicação via canal oficial acordado.
9	Recusa injustificada em executar ordens, determinações ou orientações da fiscalização.	Imediato	Multa de **2%** sobre o valor total do Contrato.	Pode configurar inexecução parcial ou total.
10	Reincidência em qualquer das ocorrências acima no período de 12 meses.	-	Multa adicional de **2%** sobre o valor total do Contrato e possibilidade de **suspensão de contratar** com a Administração por até 2 anos.	Contabiliza reincidência da mesma natureza.

tabela 1.2

9.20. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

9.20.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.20.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

9.20.3. Todas as penalidades observarão o contraditório e ampla defesa (art. 158, Lei nº 14.133/2021).

9.20.4. As glosas e multas não são excludentes, podendo ser aplicadas cumulativamente quando houver dano material e descumprimento contratual.

9.20.5. As multas poderão ser descontadas de pagamentos devidos, cobradas via retenção ou compensação financeira.

9.20.6. Em caso de reincidência ou gravidade, poderá ser proposta a rescisão unilateral do contrato e aplicação das sanções de impedimento e inidoneidade.

9.21. **LIQUIDAÇÃO**

9.22. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

9.23. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021 .

9.24. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.24.1. o prazo de validade;

9.24.2. a data da emissão;

9.24.3. os dados do contrato e do órgão contratante;

9.24.4. o período respectivo de execução do contrato;

9.24.5. o valor a pagar; e

9.24.6. eventual destaque do valor de retenções tributárias cabíveis.

9.25. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

9.26. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

9.27. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

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

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

9.30. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

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

9.32. **PRAZO DE PAGAMENTO**

9.33. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.34. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice *IPCA-E* de correção monetária.

9.35. **FORMA DE PAGAMENTO**

9.36. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

9.39. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.40. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.41. **ANTECIPAÇÃO DE PAGAMENTO**

9.41.1. A presente contratação permite a antecipação parcial de pagamento, restrita exclusivamente aos Itens 1, 2, 3 e 4 — correspondentes ao licenciamento de software para Gestão de Vulnerabilidades, Gestão de Vulnerabilidades para Aplicações Web, Gestão de Superfície de Ataque e Gestão de Vulnerabilidades para *Active Directory*, todos com vigência de 36 (trinta e seis) meses —, desde que devidamente justificada pela contratada e aprovada pela Administração, nos termos do art. 145 da Lei nº 14.133/2021 e do art. 43 da Instrução Normativa SEGES/ME nº 77/2022.

9.41.2. A justificativa apresentada pela contratada deverá demonstrar, de forma objetiva, a necessidade da antecipação em razão de variações cambiais, políticas comerciais do fabricante ou outros fatores de mercado que impactem o custo do licenciamento, acompanhada de documentação comprobatória.

9.41.3. O pagamento antecipado estará condicionado à prestação de garantia adicional, nas modalidades previstas no art. 96 da Lei nº 14.133/2021, correspondente a 10% (dez por cento) do valor total a ser antecipado, a ser apresentada antes da liberação do pagamento.

9.41.4. A contratada emitirá nota fiscal ou fatura correspondente ao valor da antecipação, tão logo seja formalmente aprovado o pedido de antecipação pela Administração e prestada a garantia adicional exigida, para que o Confea efetue o pagamento antecipado.

9.41.5. O pagamento antecipado será efetuado no prazo máximo de até 10 (dez) dias úteis, contados do recebimento da respectiva nota fiscal ou fatura, observadas as retenções tributárias cabíveis.

9.41.6. A liquidação ocorrerá de acordo com as regras previstas na seção específica deste Termo de Referência.

9.41.7. Em caso de inexecução total do contrato, o contratado será obrigado a devolver, com correção monetária, a integralidade do valor antecipado. No caso de inexecução parcial, deverá devolver a parcela proporcional ao valor não executado, devidamente atualizada.

9.41.8. O valor relativo à parcela antecipada e não executada será atualizado monetariamente pela variação acumulada do IPCA-E (Índice Nacional de Preços ao Consumidor Amplo Especial), ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da efetiva devolução.

9.41.9. O pagamento antecipado dispensa o ateste ou recebimento prévios do objeto, os quais deverão ocorrer após a regular execução da parcela contratual correspondente ao valor antecipado.

9.41.10. A concessão de antecipação não afasta a possibilidade de aplicação de penalidades contratuais, caso se verifique descumprimento das obrigações assumidas pela contratada.

9.42. **CESSÃO DE CRÉDITO**

9.43. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

9.43.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

9.44. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

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

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

9.47. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

10.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

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

lote.

10.2. **REGIME DE EXECUÇÃO**

10.2.1. O regime de execução do contrato será empreitada por *preço unitário.*

10.3. **DA APLICAÇÃO DA MARGEM DE PREFERÊNCIA**

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

10.4. **EXIGÊNCIAS DE HABILITAÇÃO**

10.5. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

10.5.1. **HABILITAÇÃO JURÍDICA:**

10.5.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.5.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.5.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

10.5.1.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.5.1.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.5.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.5.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

10.5.2. **HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA:**

10.5.3. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.5.4. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.5.5. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.5.6. 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;

10.5.7. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] ou [Municipal/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.5.8. Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.5.9. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.5.10. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.5.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da

consolidação respectiva.

10.5.12. **Qualificação Econômico-Financeira**

10.5.13. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

10.5.14. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº14.133, de 2021, art. 69, caput, inciso II);

10.5.15. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

10.5.16. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1(um);

10.5.17. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

10.5.18. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

10.5.19. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.5.20. Caso a empresa licitante apresente resultado igual ou inferior a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Liquidez Corrente (LC) ou Solvência Geral (SG), será exigido, para fins de habilitação econômico-financeira, patrimônio líquido mínimo equivalente a até 10% (dez por cento) do valor total estimado da contratação ou, quando cabível, do valor da parcela pertinente ao objeto licitado, conforme previsão do art. 69, §2º, da Lei nº 14.133/2021 e do art. 6º, §1º, inciso III, da Instrução Normativa SEGES/ME nº 116/2021.

10.5.21. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

10.5.22. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.5.23. **QUALIFICAÇÃO TÉCNICA**

10.5.24. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;

10.5.25. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação;

10.5.26. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

10.5.27. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

10.5.28. A licitante deverá apresentar, no mínimo, 1 (um) Atestado de Capacidade Técnica emitido por pessoa jurídica de direito público ou privado, comprovando que ela forneceu solução ou prestação de serviço compatível com o objeto desta contratação emitido em papel timbrado, com assinatura, identificação e telefone do emitente.

10.5.29. Para remover a subjetividade da análise o(s) atestado(s) de capacidade técnica deverá(ão) comprovar que a licitante possui experiência prévia na solução ofertada, englobando no mínimo, 50% da volumetria e complexidade técnica de 2 (dois) tipos distintos de licenças descritas neste Termo de Referência.

10.5.30. Para o contexto de serviços solicitados, será admitida a apresentação de atestados que comprovem a execução e serviços de implantação e treinamento na solução.

10.5.31. Serão aceitos atestados de capacidade técnicas emitidos em nome da matriz ou da filial da licitante, desde que seja comprovado que elas representam a mesma entidade jurídica.

10.5.32. Serão aceitos atestados de capacidade técnica com períodos de contratação distintos desta a ser vigorada neste processo licitatório.

10.5.33. Para fins de validação, a CONTRATANTE poderá diligenciar os atestados e seus respectivos contratos firmados entre as partes.

10.5.34. As atividades que comprovam a qualificação técnico-operacional deverão se referir a serviços prestados no âmbito de sua atividade econômica principal e/ou secundária conforme especificada no contrato

social, devidamente registrado na junta comercial competente, bem como no cadastro de pessoas jurídicas da Receita Federal do Brasil - RFB.

10.5.35. **COMPROVAÇÃO TÉCNICA POR ITEM**

10.5.36. Para fins de habilitação técnica e conformidade com as especificações deste Termo de Referência, será obrigatória a comprovação técnica individualizada por item proposto. Cada item ofertado deverá estar acompanhado de documentação técnica (tais como catálogos, manuais, fichas técnicas ou declarações do fabricante), que comprove, de forma clara e objetiva, o atendimento a todos os requisitos estabelecidos nas especificações técnicas correspondentes.

10.5.37. Essa exigência tem por objetivo assegurar a aderência das propostas ao escopo técnico definido, evitar ambiguidades interpretativas e garantir a entrega de soluções compatíveis com os padrões mínimos de desempenho, funcionalidade e interoperabilidade requeridos.

10.5.38. A ausência de comprovação técnica adequada em qualquer item poderá ensejar a desclassificação parcial ou total da proposta, conforme avaliação da equipe técnica responsável.

10.5.39. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.5.40. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

10.5.41. **Disposições gerais sobre habilitação**

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

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

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

10.5.45. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de R$48.309.363,34 (quarenta e oito milhões, trezentos e nove mil trezentos e sessenta e três reais e trinta e quatro centavos).

11.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre contratante e contratado, conforme especificado na matriz de risco constante do Contrato.

11.3. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

11.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

11.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

11.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

11.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

12. REAJUSTE

12.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contados da data

do orçamento encaminhado pelas empresas, a saber: **07/01/2026**, podendo ser prorrogado nos moldes da legislação vigente.

12.2. Após o interregno de um ano, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

12.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

12.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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

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

12.8. O reajuste será realizado por apostilamento.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta "Serviços de Informática".

13.2. **CRONOGRAMA FÍSICO FINANCEIRO**

13.3. A execução do contrato seguirá o cronograma físico-financeiro a seguir descrito, observando-se as etapas técnicas, os marcos de entrega e o respectivo desembolso financeiro proporcional à execução dos serviços.

13.4. Etapa 1 – Planejamento e mobilização inicial:

13.5. Corresponde à fase preparatória do projeto, abrangendo a reunião de abertura, definição do cronograma detalhado, validação de escopo, levantamento de pré-requisitos e apresentação do plano de implantação pela contratada.

13.6. Prazo: até 10 (dez) dias após a assinatura do contrato.

13.7. Desembolso: Nesta fase, não haverá desembolso financeiro, por se tratar de etapa preparatória.

13.8. Etapa 2 – Serviço de Instalação (Item 5)

13.9. Execução dos serviços especializados de instalação, configuração, integração e testes iniciais das soluções contratadas.

13.10. Etapa 3 – Implantação dos Licenciamentos (Itens 1, 2, 3 e 4)

13.11. Após a conclusão da instalação, serão efetivadas as ativações e disponibilizações dos licenciamentos das plataformas contratadas, contemplando:

13.11.1. Gestão de Vulnerabilidades;

13.11.2. Gestão de Vulnerabilidades de Aplicações Web;

13.11.3. Gestão de Superfície de Ataque;

13.11.4. Gestão de Vulnerabilidades para Active Directory;

13.12. Etapa 4 – Início do Serviço Continuado (Item 7)

13.13. Concluída a implantação das soluções, terá início o serviço continuado de gestão de vulnerabilidades, suporte técnico e acompanhamento operacional, cuja vigência contratual passará a correr a partir desta etapa.

13.14. Etapa 5 – Treinamento (Item 6)

13.15. Realização das capacitações previstas, garantindo a transferência de conhecimento e a autonomia operacional da equipe técnica do Contratante.

13.16. Etapa 6 – Encerramento e recebimento definitivo:

13.17. Consiste na entrega do relatório final consolidado de desempenho da solução, contendo as métricas operacionais, indicadores de disponibilidade e evolução da postura de segurança do Confea durante a

vigência contratual. O recebimento definitivo ocorrerá após a validação técnica e administrativa pela fiscalização.

13.18. Prazo: até 10 (dez) dias antes o término da vigência contratual.

13.19. Desembolso: sem parcela adicional, uma vez que as obrigações financeiras já estarão incluídas nas parcelas mensais do serviço continuado.

Item	Descrição resumida	Valor médio entre as propostas	% sobre o total aproximado
1	Gestão de Vulnerabilidades (ativos)	**≈ R$ 1,23 milhão**	**≈ 47%**
2	*Aplicações Web*	≈ R$ 39 mil	≈ 1,5%
3	Superfície de Ataque	≈ R$ 58 mil	≈ 2%
4	*Active Directory*	≈ R$ 681 mil	≈ 26%
5	Instalação	≈ R$ 221 mil	≈ 8%
6	Treinamento	≈ R$ 121 mil	≈ 4,5%
7	Serviço Continuado	≈ R$ 276 mil	≈ 10,5%
Total		**≈ R$ 2,63 milhões**	**100%**

13.20. **De acordo com o art. 12, § 6º da Instrução Normativa SGD/ME nº 94, de 2022, o Termo de Referência deverá ser assinado pela Equipe de Planejamento da Contratação (Integrante Requisitante, Integrante Técnico e Integrante Administrativo) e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.**

13.21. O Termo de Referência deverá ser devidamente aprovado pelo ordenador de despesas ou a autoridade competente respectiva, conforme divisão de atribuições de cada órgão.

13.22. Registre-se que, salvo no caso de elaboração do TR pela própria autoridade competente para aprová-lo, eventual equipe incumbida de tal confecção deve ser designada pela autoridade competente nos termos do art. 7º da Lei nº 14.133, de 2021, incumbindo a esta aferir o cumprimento dos requisitos necessários a esta função.

13.23. Conforme art. 8º da IN Seges/ME nº 81, de 2022, incumbe, conjuntamente, aos servidores da área técnica e da requisitante, designados na forma do art. 7º da Lei nº 14.133, de 2021 pelas respectivas autoridades, a elaboração do Termo de Referência, podendo a mesma área cumprir ambos os papéis (art. 3º, § 2º da IN). Uma outra possibilidade é o uso de uma Equipe de Planejamento da Contratação, caso haja alguma designada para tal fim.

13.24. Atentar para a necessidade de avaliação quanto à pertinência de classificar o TR nos termos da Lei n. 12.527, de 2011 (Lei de Acesso à Informação), conforme previsão do artigo 10 da Instrução Normativa nº 81, de 2022.

14. ANEXO II - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

O **CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA**, sediado em Brasília – DF, SEPN Comércio Residencial Norte 508 - Asa Norte, Brasília/DF, 70740-541, CNPJ 33.665.647/0001-91, doravante denominada CONTRATANTE, e, de outro lado, a empresa <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO Nº <XX/XXXX> 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, referente ao Pregão Eletrônico nº XXX/2021, 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 dos CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, 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 deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO.

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.

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, tais 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 ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

CLÁUSULA NONA – DO FORO

A CONTRATANTE elege o foro de Brasília, 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 (duas) vias de igual teor e um só efeito.

De acordo:

CONTRATANTE	**CONTRATADA**	**TESTEMUNHA 1**	**TESTEMUNHA 2**
_____	_____	_____	_____
Fiscal do Contrato	Preposto	Nome/Qualificação	Nome/Qualificação

Brasília, _____ de _____ de 20_____.

15. ANEXO III - TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

TERMO DE CIÊNCIA DE MANUTENÇÃO DE SIGILO

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 N°	
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.

CIÊNCIA
CONTRATADA - Funcionários

_____	_____
Nome/CPF	Nome/CPF
_____	_____
Nome/CPF	Nome/CPF

_____ _____
Nome/CPF Nome/CPF

Brasília, _____ de _____ de 20_____.

16. ANEXO IV - TERMO DE RECEBIMENTO PR OVISÓRIO (TRP)

TERMO DE RECEBIMENTO PROVISÓRIO (TRP)

IDENTIFICAÇÃO

Pregão Eletrônico nº: XX/20XX.

Contrato nº: XXX/20XX.

Período da Vigência: O contrato terá vigência de XX (por extenso) meses, contados da data da assinatura do contrato pelo contratante, podendo ser prorrogado nos moldes da legislação vigente, ou seja, de DIA/MÊS/ANO a DIA/MÊS/ANO.

Nota de Empenho: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

Contratante: Conselho Federal de Engenharia e Agronomia - Confea

Contratada:

CNPJ:

Endereço:

Endereço Eletrônico:

Ordem de Serviço nº: XX/20XX (SEI nº XXX)

Objeto:

Valor dos Bens/Serviços Recebidos: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

Data da Entrega: DIA/MÊS/ANO.

Data do Recebimento: DIA/MÊS/ANO.

Documentos Entregues

SEI nº XXX: nome do documento.

SEI nº XXX: nome do documento.

SEI nº XXX: nome do documento.

TERMOS

Por este instrumento, atesto, para fins de cumprimento do disposto no art. 33, inciso I, da Instrução Normativa nº 94, de 23 de dezembro de 2022, que os serviços e/ou bens integrantes da Ordem de Serviço acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos, **provisoriamente**, nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato pelo contratante.

Ressaltamos que o recebimento definitivo destes serviços e/ou bens ocorrerá em até 10 (dez) dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Contrato acima identificado.

17. ANEXO V - TERMO DE RECEBIMENTO DEFINITIVO (TRD)

TERMO DE RECEBIMENTO DEFINITIVO (TRD)

IDENTIFICAÇÃO

Pregão Eletrônico nº: XX/20XX.

Contrato nº: XXX/20XX.

Período da Vigência: O contrato terá vigência de XX (por extenso) meses contados da data da assinatura do contrato pelo contratante, podendo ser prorrogado nos moldes da legislação vigente, ou seja, de DIA/MÊS/ANO a DIA/MÊS/ANO.

Nota de Empenho: Nota de inscrição em restos a pagar nº XX (SEI nº XXXX), no valor de R$ XX (por extenso).

Contratante: Conselho Federal de Engenharia e Agronomia - Confea.

Contratada:

CNPJ:

Endereço:

Endereço Eletrônico:

Ordem de Serviço nº: XX/20XX (SEI nº XXX)

Objeto:

Valor dos Bens/Serviços Recebidos: R$ XX (por extenso), com pagamentos anuais no valor de R$ XX (por extenso).

Data da Entrega: DIA/MÊS/ANO.

Data do Recebimento: DIA/MÊS/ANO.

TERMOS

Por este instrumento, em **caráter definitivo**, atestamos que os serviços e/ou bens acima identificados foram devidamente executados/entregues e atendem às exigências especificadas no Contrato nº XX/20XX (SEI nº XXXX).

De forma a subsidiar este Termo de Recebimento Definitivo - TRD, foram considerados as seguintes análises e documentos:

Termo de Recebimento Provisório (SEI nº XXXX e documentos correlatos).

Análise Técnica do Fiscal do Contrato (SEI nº XXXX documento correlatos).

Documento assinado eletronicamente por **Vinicius de Assis Lima**, **Gerente de Soluções Internas**, em 01/04/2026, às 11:22, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo de Oliveira Coelho Santos**, **Integrante Técnico**, em 01/04/2026, às 11:27, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alberto de Azevedo Santos**, **Integrante Administrativo**, em 01/04/2026, às 11:28, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://confea.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1514004** e o código CRC **9B6DA730**.

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO DE TIC

Processo: 00.003608/2024-71
Tipo de Processo: Aquisição/Contratação: Bens ou Serviços (Inclusive Licitações)
Assunto: Fornecimento de Software/Serviço de Gestão de Vulnerabilidades
Interessado: Setor de Infraestrutura e Arquitetura

1. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1.1. Contratação de solução de tecnologia da informação e comunicação para gerenciamento de exposição, compreendendo licenciamento de software, serviços especializados, suporte técnico, treinamento e serviços continuados, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

2.1. Nos termos da **Portaria nº 230/2024** (doc. 0965284), foi instituída a Equipe de Planejamento da Contratação, composta pelos seguintes empregados:

2.1.1. Vinícius de Assis Lima, matrícula nº 0745 – Integrante Requisitante;

2.1.2. Marcelo de Oliveira Coelho Santos, matrícula nº 0305 – Integrante Técnico;

2.1.3. Carlos Alberto de Azevedo Santos, matrícula nº 0753 – Integrante Administrativo.

2.2. As atribuições da Equipe de Planejamento da Contratação são aquelas estabelecidas na **Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.**

3. NECESSIDADE DA SOLUÇÃO DE TI

3.1. NECESSIDADES DE NEGÓCIO

3.1.1. Os ataques contra sistemas de informação têm se tornado cada vez mais frequentes e sofisticados em todo o mundo, e no Conselho Federal de Engenharia e Agronomia (Confea) não é diferente. A tendência observada no cenário global indica que tanto a quantidade quanto a severidade dessas ocorrências irão aumentar de forma expressiva nos próximos anos, ampliando significativamente a superfície de risco a que estão submetidas as organizações públicas e privadas.

3.1.2. Nesse contexto, a cibersegurança deixou de ser apenas uma prática recomendada e tornou-se um requisito estratégico para a continuidade das operações institucionais. As ameaças evoluíram além dos métodos clássicos - como *phishing*, *malwares* e vírus de propagação simples - para incluir ataques cada vez mais complexos, como a exploração de vulnerabilidades *zero-day* em *softwares*, campanhas de engenharia social altamente direcionadas e ações de *ransomware*, que sequestram dados críticos mediante pedido de resgate. Tais cenários evidenciam que proteger apenas a camada perimetral já não é suficiente: é imprescindível adotar práticas estruturadas de Gestão de Vulnerabilidades, capazes de identificar, priorizar e corrigir falhas antes que estas sejam exploradas por agentes maliciosos.

3.1.3. Para garantir a integridade, a confidencialidade e a disponibilidade das informações, bem como a continuidade dos negócios, o Confea mantém um Sistema de Gestão de Segurança da Informação (SGSI), que contempla a definição de papéis, responsabilidades, políticas, normas e procedimentos de segurança de TIC. Esse sistema pressupõe, entre outras medidas, o monitoramento constante, a realização de testes periódicos e a implementação de ações corretivas diante de incidentes ou deficiências identificadas. Dentro desse escopo, o processo de Gestão de Vulnerabilidades desponta como um dos pilares mais relevantes, pois permite a antecipação e mitigação de riscos em um ambiente de ameaças cibernéticas em constante transformação.

3.1.4. A implementação desse processo envolve diferentes etapas: inicia-se pela identificação de ativos de TI - servidores físicos e virtuais, estações de trabalho, *notebooks*, dispositivos móveis, *appliances* de segurança, equipamentos de rede (*switches*, roteadores, *firewalls*), bancos de dados, aplicações *web*, sistemas críticos, entre outros. No caso do Confea, o parque tecnológico conta atualmente com mais de 700 ativos de diferentes naturezas, o que torna o ambiente altamente dinâmico, interconectado e complexo de gerenciar. Essa complexidade acarreta enormes desafios, sobretudo na detecção e tratamento de vulnerabilidades técnicas que surgem continuamente devido a fatores como:

3.1.4.1. falhas de configuração;

3.1.4.2. ausência de *patch management* adequado;

3.1.4.3. *bugs* de *software* não corrigidos;

3.1.4.4. portas e serviços expostos indevidamente;

3.1.4.5. uso de credenciais fracas;

3.1.4.6. ambientes legados e desatualizados;

3.1.4.7. entre outras fragilidades.

3.1.5. Para enfrentar esse cenário, as ferramentas automatizadas de *scanner* de vulnerabilidades desempenham papel central, pois realizam varreduras abrangentes em busca de brechas de segurança, analisando códigos, configurações e comunicações de rede. Essas soluções permitem identificar rapidamente vulnerabilidades conhecidas em grande escala, fornecendo uma visão ampla do nível de exposição e facilitando a tomada de decisões proativas para mitigação.

3.1.6. Após a identificação das vulnerabilidades, torna-se essencial avaliar o risco associado a cada uma delas. Esse processo de análise considera fatores como:

3.1.6.1. impacto potencial sobre os ativos e serviços críticos;

3.1.6.2. probabilidade de exploração por agentes de ameaça;

3.1.6.3. recursos disponíveis para a mitigação.

3.1.6.4. Com base nessa avaliação, é possível priorizar correções de forma racional, destinando esforços primeiro às vulnerabilidades mais críticas. As medidas de mitigação podem incluir a aplicação de *patches* de segurança, ajustes de configuração, atualizações de *software* ou ainda a implementação de controles compensatórios quando a correção imediata não for possível.

3.1.7. Entretanto, a gestão de vulnerabilidades não se encerra com a correção inicial. É indispensável verificar a efetividade das medidas adotadas, monitorar continuamente o ambiente e realizar revisões periódicas do processo, de modo a identificar oportunidades de melhoria e garantir sua eficácia

contínua. Dessa forma, a gestão de vulnerabilidades deve ser entendida como um ciclo permanente e iterativo, que acompanha a evolução tecnológica e as mudanças no panorama das ameaças cibernéticas.

3.1.8. Além das boas práticas de governança em segurança, o Confea fundamenta suas ações em normativos legais e regulatórios vigentes, com destaque para a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), que estabelece princípios e obrigações para o tratamento seguro das informações pessoais. O alinhamento à LGPD e a outros normativos governamentais reforça a necessidade de processos estruturados de prevenção, capazes de reduzir a exposição a incidentes e assegurar o cumprimento das obrigações legais.

3.1.9. Assim, a contratação de uma solução de Gestão de Vulnerabilidades justifica-se como medida essencial para fortalecer a postura de segurança do Confea, assegurando a proteção dos ativos institucionais, a conformidade legal e regulatória, a redução de riscos e a preservação da confiança dos usuários internos e externos na integridade dos serviços prestados.

3.2. **NECESSIDADES TÉCNICAS**

3.2.1. A solução a ser contratada deve possibilitar a gestão contínua de vulnerabilidades e da exposição a ameaças, de forma proativa e recorrente. Isso implica a adoção de práticas sistemáticas de identificação, avaliação, categorização, priorização, tratamento e análise crítica das vulnerabilidades e riscos de segurança que afetam os ativos corporativos de Tecnologia da Informação e Comunicação (TIC). A abordagem deve abranger tanto o gerenciamento da superfície de ataque interna e externa quanto a análise de exposição a ameaças, permitindo uma visão integrada do nível de risco cibernético da instituição.

3.2.2. Para atingir esse objetivo, torna-se imprescindível a utilização de ferramenta especializada capaz de:

3.2.2.1. realizar varreduras e avaliações abrangentes de vulnerabilidades;

3.2.2.2. verificar a conformidade das configurações de ativos de acordo com normas e padrões reconhecidos;

3.2.2.3. fornecer mecanismos de priorização de riscos que orientem a tomada de decisão gerencial.

3.2.2.4. Descoberta e identificação de ativos;

3.2.2.5. A solução deve realizar a descoberta automática e a identificação detalhada dos ativos presentes no ambiente corporativo do Confea, analisando suas configurações sob os critérios de segurança, conformidade e aderência a normas, frameworks e bases de conhecimento internacionalmente reconhecidos. Além disso, deve possibilitar o estabelecimento de linhas de base de configuração, permitindo o rastreamento de alterações e a detecção de desvios que possam comprometer a segurança.

3.2.3. Amplitude de cobertura;

3.2.4. O processo de gestão de vulnerabilidades deve abranger de forma ampla os ativos de TIC da instituição, incluindo:

3.2.4.1. dispositivos de usuário final (estações de trabalho, notebooks, periféricos e dispositivos móveis);

3.2.4.2. dispositivos de rede (switches, roteadores, firewalls e appliances de segurança);

3.2.4.3. dispositivos inteligentes conectados à rede, como relógios de ponto eletrônico e outros equipamentos de Internet das Coisas – IoT;

3.2.4.4. servidores físicos e virtuais, contêineres e sistemas operacionais;

3.2.4.5. aplicações corporativas e serviços em rede;

3.2.4.6. ativos e posturas de segurança em ambientes de nuvem.

3.2.5. A diversidade e heterogeneidade do parque tecnológico do Confea demandam uma solução que consiga atuar de forma transversal, contemplando desde a camada de usuário até a infraestrutura crítica.

3.2.6. Varreduras de vulnerabilidade;

3.2.6.1. Devem ser realizadas varreduras automatizadas de vulnerabilidades em ativos internos e externos com periodicidade mínima trimestral, incluindo a repetição das varreduras após a aplicação de patches, atualizações e demais salvaguardas.

3.2.6.2. As varreduras devem contemplar tanto abordagens autenticadas quanto não autenticadas, garantindo profundidade e abrangência.

3.2.6.3. A solução deve apresentar compatibilidade, no mínimo, com o protocolo Security Content Automation Protocol – SCAP, de modo a assegurar padronização e confiabilidade.

3.2.6.4. Quando devidamente calibradas, as varreduras automatizadas conduzidas por agentes e pela rede externa devem ter como meta a periodicidade diária, enquanto as varreduras da rede interna devem ocorrer em ciclos mensais ou quinzenais, observando-se os períodos de gestão de patches e os impactos em desempenho, disponibilidade e tráfego de rede.

3.2.7. Priorização baseada em risco;

3.2.8. A ferramenta deve incluir tecnologia de Vulnerability Prioritization Technology (VPT), baseada em risco e altamente adaptável. Essa priorização deve levar em consideração, de forma combinada:

3.2.8.1. a severidade das vulnerabilidades identificadas;

3.2.8.2. a criticidade dos ativos e serviços afetados;

3.2.8.3. o contexto dinâmico das ameaças (existência e atividade de exploits).

3.2.8.4. Esse modelo de priorização orienta a destinação de esforços para as vulnerabilidades que representam maior risco efetivo ao negócio, otimizando recursos e fortalecendo a resiliência organizacional.

3.2.9. Integração com inteligência de ameaças;

3.2.10. A solução deve agregar recursos de Threat Intelligence, permitindo o rastreamento do uso ativo de vulnerabilidades e sua priorização com base em diferentes níveis de inteligência:

3.2.10.1. estratégico: relatórios, bases de conhecimento e fontes abertas, incluindo Deep Web e Dark Web;

3.2.10.2. tático: correlação com táticas, técnicas e procedimentos (TTPs) de adversários;

3.2.10.3. operacional: correlação com indicadores de comprometimento (IOCs).

3.2.10.4. A inteligência de ameaças deve ser proveniente tanto do fabricante da ferramenta quanto de fontes abertas e, adicionalmente, da própria contratada, ampliando a qualidade e diversidade das informações utilizadas no processo decisório.

3.2.11. Acompanhamento de referências e melhores práticas;

3.2.12. A solução deve contemplar o acompanhamento constante de alertas de segurança, atualizações, referenciais de vulnerabilidades e boas práticas de hardening para ativos de TIC, com base em repositórios e padrões amplamente reconhecidos, tais como:

3.2.12.1. NIST National Vulnerability Database (NVD);

3.2.12.2. MITRE Common Vulnerabilities and Exposures (CVE);

3.2.12.3. NIST Official Common Platform Enumeration (CPE);

3.2.12.4. MITRE Common Weakness Enumeration (CWE);

3.2.12.5. OWASP Top 10;

3.2.12.6. CIS Benchmarks.

3.2.12.7. Além disso, devem ser considerados os repositórios e centros de segurança dos principais fabricantes de tecnologia aplicáveis aos ativos do Confea, contemplando no mínimo: Microsoft, Oracle, Google, Red Hat, Dell/EMC, HP/Aruba, Check Point, F5 Networks, Broadcom/Symantec, VMware, Micro Focus, Commvault, Cisco, Mozilla e Adobe.

3.3. **NECESSIDADE DA SOLUÇÃO DE TI – QUANTITATIVO ESTIMADO**

3.3.1. Como detalhado no diagnóstico, a presente contratação visa elevar o nível de segurança do parque tecnológico do Confea, assegurando cobertura adequada para a gestão contínua de vulnerabilidades, monitoramento de exposição e redução de riscos.

3.3.2. Para dimensionar a demanda ao longo do horizonte contratual de 36 (trinta e seis) meses, adota-se a projeção exponencial com taxa anual constante, conforme a fórmula:

Y = X × (1 + i)^n, em que Y é o valor projetado, X o valor de referência atual, i a taxa de crescimento anual (em decimal) e n o número de anos (36 meses = 3 anos).

3.3.3. Essa abordagem é amplamente utilizada em estimativas de demanda, capacidade, base de usuários, custos operacionais e volume de dados, e fundamenta a escalabilidade da solução a ser contratada.

3.3.4. *Gestão de vulnerabilidades para Active Directory (AD);*

3.3.4.1. Considerando o cenário atual de 420 usuários e o objetivo de alcançar 480 licenças ao fim de 36 meses, a taxa originalmente indicada (3% a.a.) não conduz ao total pretendido, pois resultaria em aproximadamente 459 usuários projetados ($420 \times 1{,}03^3 \approx 458{,}9$). Para aderir ao quantitativo final, recalibra-se a taxa anual para ≈ 4,55% a.a. ($i \approx 0{,}0455$), de modo que $420 \times (1 + 0{,}0455)^3 \approx 480$.

3.3.4.2. Assim, fixa-se o quantitativo projetado em 480 licenças para cobertura de usuários vinculados ao AD, habilitando a identificação tempestiva de vulnerabilidades relacionadas a controladores de domínio, políticas e configurações, e mitigando riscos no período de vigência contratual. Recomenda-se o monitoramento contínuo da utilização e a reavaliação semestral da curva de crescimento, para eventuais ajustes finos sem prejuízo da cobertura.

3.3.5. *Gestão de Vulnerabilidades (parque de ativos);*

3.3.5.1. Partindo de 437 ativos atualmente mapeados e adotando crescimento de 10% a.a. por 36 meses, a projeção resulta em ≈ 582 ativos ($437 \times 1{,}10^3 \approx 581{,}6$). Para evitar *subdimensionamento*, recomenda-se arredondamento para o inteiro superior, fixando 582 licenças.

3.3.5.2. Esse patamar assegura descoberta contínua e ativa de todos os ativos de TI, com visibilidade abrangente do ambiente e identificação de lacunas com alta probabilidade de exploração e impacto ao negócio. A priorização deve combinar gravidade (CVSS), criticidade do ativo/serviço e contexto de ameaças (exploração ativa), de modo a orientar correções, medir tendências de remediação e comparar progresso internamente.

3.3.6. *Gestão de superfície de ataque (externa);*

3.3.6.1. Com base em 31 alvos atualmente identificados e aplicando 10% a.a. por 3 anos, projeta-se ≈ 41,3; adota-se 42 licenças (arredondamento para cima) para cobrir variações e novos vetores. O objetivo é mapear e rastrear, de forma contínua, ativos expostos na Internet (via DNS, endereços IP e ASN), provendo alertas de mudança na superfície de ataque e mitigando exposições decorrentes de novas publicações de serviços, reconfigurações ou ativos órfãos.

3.3.7. *Gestão de vulnerabilidades em aplicações web;*

3.3.7.1. Partindo de 16 aplicações, com 10% a.a. por 36 meses, obtém-se ≈ 21,3; recomenda-se 22 licenças (arredondamento para o inteiro superior) para descoberta contínua e ativa de aplicações *web*, com visibilidade em tempo quase real e detecção de fraquezas alinhadas a OWASP Top 10 e outras referências, priorizando correções nas vulnerabilidades de maior risco.

3.3.8. *Nota metodológica e de Governança;*

3.3.8.1. Para todos os grupos, adota-se como regra arredondamento para o inteiro superior, prevenindo *subdimensionamento* diante de variações de inventário, novos projetos, migrações para nuvem, integrações sistêmicas e picos de demanda.

3.3.8.2. O crescimento é tratado como taxa anual constante, revisável a cada ciclo de gestão (p.ex., semestral) à luz de métricas observadas (ativos descobertos, taxa de depreciação/aposentadoria, criação de novos serviços).

3.3.8.3. A contratação deverá prever relatórios periódicos contendo:

3.3.8.4. i) inventário e variações por família de ativos;

3.3.8.5. ii) vulnerabilidades críticas identificadas, tempo médio de correção e tendências de remediação;

3.3.8.6. iii) exposições externas emergentes e tratativas; iv) indicadores de risco e priorização baseada em evidências (vulnerabilities + *threat intelligence* + contexto do ativo).

3.3.8.7. Caso a métrica contratual final não seja por usuário/ativo (p.ex., licenças por *endpoint*, por scanner, por volume de IPs ou por aplicação), os quantitativos projetados permanecem válidos como *baseline* técnico, devendo apenas ser mapeados para a unidade de medida comercial do fornecedor no momento da estimativa de custos.

Escopo	Base Atual	Taxa Anual	Projeção (36 meses)	Arredondamento	Total Estimado
Gestão de Vulnerabilidades – Active Directory	420 usuários	~4,55%	≈ 480,0	—	**480 licenças**
Gestão de Vulnerabilidades – Ativos de TI	437 ativos	10%	≈ 581,6	↑	**582 licenças**
Gestão de Superfície de Ataque	31 ativos	10%	≈ 41,3	↑	**42 licenças**
Gestão de Vulnerabilidades *Web*	16 apps	10%	≈ 21,3	↑	**22 licenças**

3.4. **SERVIÇO DE INSTALAÇÃO ESPECIALIZADO**

3.4.1. A instalação especializada de uma solução de *Gestão de Vulnerabilidades* constitui etapa essencial para garantir sua integração eficaz ao ambiente tecnológico do Confea. Diferente de *softwares* convencionais, ferramentas dessa natureza demandam configurações específicas e criteriosas, capazes de assegurar a correta realização de varreduras em ativos heterogêneos, a detecção precisa de falhas, a classificação contextualizada dos riscos e a interoperabilidade com sistemas de autenticação, inventário e segurança já existentes.

3.4.2. A atuação de profissionais capacitados é indispensável para que scanners, agentes e sensores sejam adequadamente posicionados, configurados e validados em conformidade com as melhores práticas de segurança da informação e com os requisitos técnicos do órgão. Nessa etapa, realizam-se testes de conectividade, validação do escopo de ativos, definição de perfis de varredura, calibração de desempenho e ajustes de modo a evitar impactos negativos na infraestrutura monitorada. Também são estabelecidos parâmetros como periodicidade de análises, classificação de níveis de criticidade, envio de notificações automáticas e adequação às políticas internas de segurança, sempre em conformidade com a Lei Geral de Proteção de Dados (LGPD) e normativos correlatos.

3.4.3. A preparação do ambiente pode envolver a criação de contas de serviço específicas, ajustes de permissões em firewalls, definição de zonas seguras para análise e integração com soluções corporativas já implantadas, tais como SIEM (*Security Information and Event Management*), ITSM (*IT Service Management*) e EDR (*Endpoint Detection and Response*). A instalação especializada assegura que todas essas etapas sejam executadas com o mínimo de impacto operacional, antecipando potenciais restrições técnicas e garantindo a aderência às políticas de segurança e privacidade.

3.4.4. Além dos aspectos técnicos, a instalação especializada agrega valor ao projeto por incluir a capacitação da equipe técnica responsável pela operação da ferramenta, a produção de documentação completa da arquitetura implantada e o suporte técnico nos primeiros ciclos de utilização. Isso permite que o Confea atinja autonomia operacional na interpretação de resultados, na priorização de ações de correção e na tomada de decisão fundamentada em critérios objetivos.

3.4.5. Dessa forma, a instalação especializada deixa de ser um serviço meramente acessório e se consolida como um componente estratégico para o

sucesso da iniciativa de gestão de vulnerabilidades, garantindo que a solução seja utilizada em sua plenitude desde o início do contrato.

3.4.6. Considerando que o projeto contempla quatro módulos distintos de *Gestão de Vulnerabilidades* (Active Directory, ativos de TI, superfície de ataque e aplicações web), será previsto o mesmo quantitativo de serviços de instalação, ou seja, quatro serviços especializados de instalação, correspondentes a um para cada módulo.

3.5. **SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES**

3.5.1. A gestão de vulnerabilidades consolidou-se como um componente estratégico e indispensável para a proteção dos ativos digitais e para a manutenção da confiança institucional. Nesse sentido, a contratação de um serviço continuado de gestão de vulnerabilidades não deve ser vista apenas como suporte técnico, mas como um pilar de governança em *cibersegurança*, assegurando a efetividade e a perenidade dos processos de identificação, análise, priorização e mitigação de riscos.

3.5.2. A natureza dinâmica e imprevisível das vulnerabilidades torna inviável confiar apenas em uma implantação inicial da ferramenta. Novas falhas surgem diariamente em sistemas, aplicações e dispositivos, e a simples utilização isolada de uma plataforma, sem operação especializada contínua, limita fortemente sua eficácia. Para que a solução seja bem-sucedida, é imprescindível contar com atualização recorrente de políticas de varredura, interpretação contextualizada dos resultados e implementação tempestiva de medidas corretivas.

3.5.3. O serviço continuado assegura a realização cíclica e sistemática de varreduras, calibradas conforme a criticidade dos ativos e as especificidades do ambiente tecnológico do Confea. Além disso, viabiliza a integração efetiva da plataforma ao ecossistema de segurança da informação já existente, promovendo sinergia com soluções de SIEM, ITSM, EDR e demais controles. Essa integração favorece a correlação de eventos, a automação de respostas e a otimização dos tempos de reação, reduzindo a exposição do Confea a riscos cibernéticos.

3.5.4. Outro elemento central é a produção de relatórios estratégicos e operacionais, que não apenas apoiam as equipes técnicas, mas também subsidiam a tomada de decisão por parte da alta gestão, fornecendo insumos objetivos para avaliação de riscos, priorização de investimentos e definição de políticas institucionais de segurança.

3.5.5. A presença de uma contratada especializada agrega valor ao processo, assumindo responsabilidades que vão além da simples execução de *scans*, como:

3.5.5.1. diagnóstico e correção de inconsistências em escaneamentos;

3.5.5.2. tratamento de falsos positivos e lacunas de detecção;

3.5.5.3. reconfiguração de políticas após atualizações ou mudanças de ambiente;

3.5.5.4. análise crítica e depuração contínua dos resultados.

3.5.6. Esse ciclo de acompanhamento contínuo é o que efetivamente viabiliza a evolução da maturidade cibernética do Confea, permitindo que a instituição se mantenha alinhada às melhores práticas internacionais e às exigências normativas nacionais, como a LGPD.

3.5.7. O serviço de gestão de vulnerabilidades deverá possuir vigência durante todo o período contratual, operando de forma permanente, e será parametrizado de acordo com os quatro módulos previstos (Active Directory, ativos de TI, superfície de ataque e aplicações web), de modo que cada unidade de serviço reflita um escopo específico e autônomo dentro da plataforma contratada.

3.6. **SERVIÇO DE CAPACITAÇÃO**

3.6.1. A contratação de treinamento especializado para operação da solução de gestão de vulnerabilidades é condição fundamental para assegurar a eficácia e a segurança do ambiente digital do Confea. Diferentemente de *softwares* convencionais, ferramentas dessa natureza requerem conhecimento técnico avançado para que sejam corretamente configuradas, operadas e continuamente otimizadas. Sem capacitação adequada, há riscos concretos de subutilização de recursos críticos, interpretações equivocadas de relatórios de risco ou até negligência em processos essenciais de correção, o que poderia comprometer toda a estratégia de cibersegurança da instituição.

3.6.2. A capacitação, portanto, não apenas habilita a equipe técnica a explorar plenamente os recursos da solução, mas também fortalece a integração com outras plataformas corporativas de segurança (como SIEM, ITSM e EDR), permitindo a automação de respostas a incidentes, a criação de relatórios estratégicos e a conformidade com auditorias e normativos. Esse alinhamento contribui diretamente para o aumento da maturidade cibernética do Confea e para a prevenção de incidentes que poderiam ser evitados por meio de ações proativas.

3.6.3. Investir em capacitação também reduz a dependência de suporte externo, eleva a autonomia da equipe de TIC e resulta em uma operação mais ágil, confiável e resiliente. Em um cenário de ameaças cibernéticas em constante evolução, dispor de profissionais habilitados para utilizar integralmente uma plataforma de gestão de vulnerabilidades não é apenas um diferencial técnico, mas uma necessidade estratégica para a proteção dos ativos institucionais, para a continuidade dos serviços prestados e para a aderência a padrões de governança em segurança da informação, como a ISO/IEC 27001 e o NIST Cybersecurity Framework, além das exigências de prestação de contas previstas na Lei Geral de Proteção de Dados (LGPD).

3.6.4. Para garantir abrangência e aderência às diferentes frentes do projeto, o serviço de capacitação será parametrizado por módulo contratado, totalizando quatro unidades distintas de treinamento. Cada módulo contará com ementa própria, alinhada ao respectivo escopo funcional (Active Directory, ativos de TI, superfície de ataque e aplicações web), assegurando que o corpo técnico receba formação direcionada e aplicável à sua área de atuação.

3.7. **ALINHAMENTO ENTRE A CONTRATAÇÃO E O PDTI**

3.7.1. A contratação de solução para gestão de vulnerabilidades está alinhada às diretrizes gerais do Plano Diretor de Tecnologia da Informação (PDTI) do Confea, em especial aquelas voltadas ao fortalecimento da governança, à segurança da informação e à melhoria contínua da infraestrutura tecnológica. O PDTI 2023-2025 estabelece, entre suas prioridades, a adoção de um modelo de governança baseado em melhores práticas de mercado, a busca por aumento de produtividade, a garantia de segurança da informação e a valorização dos recursos humanos da área de TI.

3.7.2. Nesse sentido, a presente contratação contribui de forma transversal e estruturante para diversas iniciativas em curso, ao prover um mecanismo que fortalece a visibilidade, a resiliência e a conformidade do ambiente tecnológico. A solução de gestão de vulnerabilidades atua como elemento de suporte crítico para a consecução de objetivos estratégicos previstos, tais como:

3.7.3. ID 18 – Reestruturação dos servidores de Active Directory. A identificação e mitigação de vulnerabilidades em controladores de domínio é condição indispensável para assegurar que a reestruturação dos servidores de Active Directory se dê em ambiente confiável, reduzindo riscos decorrentes de objetos legados e conflitos existentes.

3.7.4. ID 23 – Security Operations Center (SOC). A gestão de vulnerabilidades complementa a atuação do SOC ao fornecer insumos qualificados sobre exposição a riscos, ampliando a capacidade de correlação de eventos e priorização de incidentes.

3.7.5. ID 25 – Solução de avaliação e tratamento de dados (LGPD). O processo de gestão de vulnerabilidades reforça a conformidade com a LGPD, na medida em que reduz o risco de incidentes de segurança que possam comprometer a confidencialidade, a integridade e a disponibilidade de dados pessoais.

3.7.6. ID 27 – Solução de inventário e gerenciamento de *endpoints*. A descoberta contínua e ativa de ativos de TI, inerente ao processo de gestão de vulnerabilidades, converge com a necessidade de inventário e gerenciamento de endpoints, fornecendo informações que subsidiam a adoção de tecnologia específica para esse fim.

3.7.7. Assim, a contratação ora proposta não apenas observa as diretrizes do PDTI 2023-2025 como também se integra a diferentes iniciativas estratégicas, atuando como fator de sustentação e catalisador para sua efetiva implementação. Com isso, reforça-se a coerência do planejamento de TI do Confea, assegurando que os investimentos realizados sejam convergentes e que os riscos de segurança cibernética sejam tratados de maneira sistêmica e coordenada.

3.8. **LEVANTAMENTO DAS SOLUÇÕES**

3.9. No processo de avaliação das alternativas tecnológicas para gestão de vulnerabilidades, foram consideradas três possibilidades principais:

3.10. **Solução 01 – Plataformas Open Source.**

3.10.1. Foram analisadas ferramentas de código aberto, como OpenVAS, Faraday, OpenSCAP e W3AF. Tais soluções apresentam como atrativos o baixo custo de aquisição e a possibilidade de personalização por meio do acesso ao código-fonte, bem como a transparência decorrente da abertura do código e a existência de comunidades ativas que promovem evolução contínua. Entretanto, por se tratarem de plataformas sem suporte formal estruturado, estas soluções tendem a demandar alta especialização da equipe interna, apresentando dificuldades em termos de escalabilidade, confiabilidade e integração a ambientes corporativos complexos. Além disso, a ausência de documentação oficial robusta e de garantias de atualização tempestiva frente a novas ameaças limita sua efetividade em cenários que exigem maturidade institucional elevada.

3.11. **Solução 02 – Desenvolvimento Interno.**

3.11.1. Outra alternativa considerada foi a criação de uma aplicação proprietária desenvolvida internamente pela equipe do Confea. Essa opção proporcionaria personalização total da solução, controle absoluto sobre a evolução do produto, independência de fornecedores e potencial flexibilidade para expansões futuras. Contudo, os desafios associados a essa abordagem são expressivos: alta demanda de tempo e recursos para desenvolvimento, necessidade de equipe multidisciplinar dedicada e custos ocultos de manutenção a médio e longo prazo. Ainda que viável teoricamente, a criação de uma solução proprietária apresenta elevado risco de atrasos, fragilidade em atualizações e obsolescência, especialmente diante da velocidade com que surgem novas vulnerabilidades no cenário global.

3.12. **Solução 03 – Ferramentas Comerciais de Mercado.**

3.12.1. As ferramentas comerciais analisadas destacam-se por oferecer funcionalidades avançadas, como painéis intuitivos, relatórios executivos, integração automatizada com ecossistemas de segurança e suporte técnico dedicado. Essas soluções são projetadas para alta escalabilidade e apresentam atualizações regulares, acompanhando as tendências de ataque e as exigências regulatórias mais recentes. Diferenciam-se, ainda, pela facilidade de uso, documentação consistente e confiabilidade assegurada por fornecedores especializados. Embora envolvam custos de licenciamento, tais investimentos são compensados pela maturidade tecnológica, pela redução de riscos operacionais e pela capacidade de resposta imediata a novas ameaças.

3.13. **Análise Comparativa:**

3.13.1. Com base nos requisitos tecnológicos mínimos indispensáveis definidos para o Confea, elaborou-se a matriz de comparação a seguir:

Requisitos	**Solução 01**	**Solução 02**	**Solução 03**
Atende	1/16	2/16	16/16
Atende Parcialmente	4/16	5/16	0/16
Não Atende	11/16	9/16	0/16

3.13.2. A análise demonstra que as soluções *open source* e proprietária interna não atendem, de forma satisfatória, ao conjunto de requisitos mínimos definidos para a contratação. A primeira enfrenta limitações de suporte, escalabilidade e confiabilidade; a segunda, riscos elevados de desenvolvimento, manutenção e obsolescência. Em contraste, as ferramentas de mercado cumprem integralmente os 16 requisitos estabelecidos, evidenciando **aderência total** às necessidades institucionais.

3.14. **Registro da Solução Considerada Viável**

3.14.1. Diante do exposto, conclui-se que a **Solução 03 – Ferramentas Comerciais de Mercado** é a mais viável para atender ao objeto desta contratação. Essa opção apresenta **menor complexidade de implantação e sustentação**, assegura aderência aos requisitos de segurança, confiabilidade e governança, e se mostra mais alinhada à realidade do Confea, especialmente considerando o aumento da sofisticação dos ataques cibernéticos e a necessidade de resposta ágil a vulnerabilidades emergentes.

3.14.2. Assim, a adoção de solução comercial de mercado garante maior eficiência, reduz riscos operacionais e possibilita a consolidação de uma postura de segurança condizente com as demandas atuais e futuras do ambiente tecnológico da instituição.

Requisitos	Solução 01	Solução 02	Solução 03
Custo de manutenção	Atende	Atende	Atende
Flexibilidade	Não Atende	Atende Parcialmente	Atende
Escalabilidade	Não Atende	Não Atende	Atende
Facilidade de uso	Não Atende	Atende Parcialmente	Atende
Velocidade de implementação	Atende Parcialmente	Atende Parcialmente	Atende
Capacidade técnica	Atende Parcialmente	Atende Parcialmente	Atende
Confiabilidade	Não Atende	Atende	Atende
Compatibilidade	Não Atende	Não Atende	Atende
Segurança	Não Atende	Atende Parcialmente	Atende
Atualização e Suporte	Atende Parcialmente	Não Atende	Atende
Documentação	Não Atende	Não Atende	Atende
Reputação	Não Atende	Não Atende	Atende
Tempo para desenvolvimento	Não Atende	Não Atende	Atende
Propriedade intelectual	Não Atende	Atende	Atende
Customização	Não Atende	Atende	Atende
Impacto	Não Atende	Não Atende	Atende

3.15. **LEVANTAMENTO DE MERCADO DA SOLUÇÃO CONSIDERADA VIÁVEL**

3.15.1. Como ponto de partida para a análise das soluções aderentes ao escopo proposto, foi considerado um levantamento baseado em estudos de mercado e publicações especializadas no setor de tecnologia, com foco na identificação dos principais fornecedores globais que oferecem esse tipo de solução. Essa abordagem permitiu uma visão abrangente do cenário atual e das tendências adotadas pelas empresas líderes do segmento;

3.15.2. A seguir, elencamos algumas fabricantes escolhidas para uma análise minuciosa de funcionalidades, de métricas de licenciamento/consumo e de demais aspectos tecnológicos necessários ao nosso escopo de contratação.

3.15.3. Com base no objeto deste processo, foi efetuado um levantamento de possíveis cenários visando seu atendimento, os quais sejam:

3.15.3.1. **SOLUÇÃO 01:** *Rapid7*;

3.15.3.2. **SOLUÇÃO 02:** *Qualys*;

3.15.3.3. **SOLUÇÃO 03:** *Tenable*.

ANÁLISE COMPARATIVA DE SOLUÇÕES SOB OS ASPECTOS QUALITATIVOS			
REQUISITOS DE NEGÓCIO	**SOLUÇÃO / CENÁRIO**		
	01	**02**	**03**
	Rapid7	**Qualys**	**Tenable**
Cobertura de vulnerabilidades	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Priorização baseada em risco	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_

Classificação de vulnerabilidades	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Serviços Profissionais	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
RESULTADO DA ANÁLISE	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
REQUISITOS TECNOLÓGICOS	**SOLUÇÃO / CENÁRIO**		
	01	**02**	**03**
Sistema de segurança de identidade	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Análise holística de SLA	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Análise de via de ataque	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Cobertura geral de ativos	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Análise de gerenciamento de Exposição	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Priorização e criticidade de ativos	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Inteligência de vulnerabilidade	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Proteção de identidade de segurança em nuvem	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Superfície de Ataques	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Container	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_
Aplicações WEB	https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brochure.pdf	https://cdn2.qualys.com/docs/mktg/vulnerability-management-datasheet-pt.pdf	https://dam.tenable.com/f402f3b141011beb81/Tenable_One_Exposu_The_only_all-enterprise_exposure_

3.15.4. Diversas ferramentas disponíveis no mercado foram avaliadas; contudo, a solução a ser adotada deverá possuir funcionalidades compatíveis com os requisitos definidos no Termo de Referência.

3.16. **REGISTRO DE SOLUÇÃO CONSIDERADA INVIÁVEL**

3.16.1. Desenvolver ou utilizar ferramentas *open source* para gestão de vulnerabilidades não é viável no momento para o CONFEA;

3.16.2. A complexidade e o custo de desenvolvimento para criar uma ferramenta exige recursos significativos, como tempo, equipe especializada e investimento financeiro. Além disso, é necessário garantir que a solução seja robusta e segura, o que pode ser desafiador.

3.16.3. Ferramentas *opensource* podem conter vulnerabilidades devido à sua natureza aberta. Projetos *opensource* são mais suscetíveis a falhas de segurança, uma vez que não há a garantia de que uma entidade desenvolve o produto de modo seguro, o que pode expor a organização a ataques cibernéticos.

3.16.4. Ferramentas *opensource* frequentemente dependem de comunidades para atualizações e suporte. Isso pode ser problemático em situações críticas, onde o suporte imediato é necessário.

3.16.5. Garantir conformidade com normas como a LGPD pode ser mais complexo em soluções *opensource*, especialmente se não houver uma equipe dedicada para realizar auditorias e ajustes necessários.

3.16.6. Ferramentas de gestão de vulnerabilidades comerciais geralmente oferecem maior capacidade de escalabilidade, permitindo que organizações cresçam sem comprometer a segurança.

3.16.7. Soluções comerciais frequentemente possuem integração nativa com outras ferramentas de segurança, como SIEMs (Security Information and Event Management), o que facilita a centralização do monitoramento.

3.16.8. Ferramentas comerciais recebem atualizações regulares para acompanhar novas ameaças e vulnerabilidades, enquanto soluções open source podem depender de comunidades que nem sempre têm recursos para atualizações rápidas.

3.16.9. Empresas que fornecem ferramentas comerciais geralmente oferecem suporte técnico especializado, garantindo assistência em situações críticas.

3.16.10. Soluções comerciais frequentemente incluem funcionalidades para atender requisitos de conformidade, como auditorias e relatórios detalhados.

3.16.11. Ferramentas comerciais podem oferecer automação mais robusta, reduzindo o esforço manual e aumentando a eficiência na gestão de vulnerabilidades.

3.17. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

3.17.1. A equipe de planejamento apresenta o quantitativo necessário para cada um dos itens previstos para uma vigência contratual de 36 (trinta e seis) meses:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	UN	580
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	UN	20
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	UN	41

4	LICENCIAMENTO PARA A GESTAO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	UN	480
5	SERVIÇO DE INSTALAÇÃO	UN	4
6	TREINAMENTO POR SOLUÇÃO	UN	4
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	UN	4

3.17.2. ITEM 1 – Licenciamento de 580 unidades de ferramenta de gestão de vulnerabilidades com validade de 36 meses;

3.17.3. ITEM 2 – Licenciamento de 20 unidades de ferramenta de gestão de vulnerabilidades para aplicações web com 36 meses de validade

3.17.4. ITEM 3 – Licenciamento de 41 unidades de ferramenta de gestão de superfície de ataque com validade de 36 meses;

3.17.5. ITEM 4 – Licenciamento de 480 unidades de ferramenta para gestão de vulnerabilidades para Active Directory com 36 meses de validade;

3.17.6. ITEM 5 – Serviço de instalação especializada, cada unidade deste item é equivalente a 1 plataforma;

3.17.7. ITEM 6 – Treinamento da solução por ferramenta;

3.17.8. ITEM 7 – Serviço continuado para gestão de vulnerabilidades com 36 meses de vigência e 4 (quatro) unidades registradas, sendo uma específica por módulo.

3.18. **LEVANTAMENTO DE MERCADO**

3.18.1. Foi efetuado levantamento para identificar quais soluções existentes no mercado atenderiam aos requisitos estabelecidos, e se há disponibilidade de prestadores de serviço, de modo a alcançar os resultados pretendidos e atender à necessidade da contratação, levando-se em conta aspectos de economicidade, eficácia, eficiência e padronização.

3.18.2. Em complemento, adotou-se como instrumento balizador a **Instrução Normativa nº 94, de 23 de dezembro de 2022**, conforme disposto em seu art. 11 que a análise comparativa de soluções deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observando:

3.18.3. **II - Análise comparativa de soluções, que deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação, observando:**

3.18.4. Os benefícios de **negócio** almejados com a contratação são:

3.18.4.1. Cumprimento de conformidades e Regulamentações;

3.18.4.2. Redução de risco de segurança;

3.18.4.3. Eficiência operacional;

3.18.4.4. Aumento da resiliência organizacional;

3.18.4.5. Redução de custo com incidentes;

3.18.4.6. Escalabilidade.

3.18.5. Os benefícios **técnicos** almejados com a contratação são:

3.18.5.1. Visibilidade total dos ativos e vulnerabilidades de rede;

3.18.5.2. Priorização baseada em risco;

3.18.5.3. Monitoramento contínuo;

3.18.5.4. Análise de risco cibernético;

3.18.5.5. Cobertura abrangente de Vulnerabilidades;

3.18.5.6. Ferramenta única para gerenciar todas as vulnerabilidades;

3.18.5.7. Segurança de identidade;

3.18.5.8. Conformidade Regulamentar.

3.19. **Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas.**

3.19.1. Conforme descrito no capítulo 13 “ESTIMATIVAS PRELIMINARES DE PREÇO”.

3.20. **As alternativas do mercado.**

3.20.1. Conforme descrito no capítulo 6“LEVANTAMENTO DE MERCADO DA SOLUÇÃO CONSIDERADA VIÁVEL”.

3.21. **A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações.**

3.21.1. A referida Portaria dispõe sobre a disponibilização de Software Público Brasileiro e dá outras providências.

3.21.2. Em consulta ao Portal do Software Público Brasileiro através da palavra-chave "Gerenciamento de Vulnerabilidades", realizada em 10/07/2024 mediante link https://softwarepublico.gov.br/social/search/software_infos, não foram encontrados softwares que atendessem o objeto pleiteado neste processo.

3.22. **As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis.**

3.22.1. Não se aplica a este Estudo Técnico Preliminar.

3.23. **A necessidade de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual.**

3.23.1. Não há necessidade de adequação do ambiente para esta contratação.

3.24. **Os diferentes modelos de prestação de serviço.**

3.24.1. Para o contexto previsto, fora computado o seguinte escopo de serviços correlatos:

3.24.2. Todas as licenças deverão incluir o processo de instalação e configuração correta da solução em conjunto ao fornecimento delas.

3.24.3. Ademais, será contabilizado o escopo de Unidades de Serviço Técnico, para a execução de atividades especializadas, sob demanda, durante a execução contratual.

3.24.4. Por fim, o serviço continuado possui o propósito de garantir a manutenção da operacionalidade, da segurança e da evolução contínua das soluções implementadas, assegurando suporte técnico especializado, atualizações regulares, monitoramento proativo e respostas rápidas a incidentes. Essa abordagem visa não apenas preservar os níveis de serviço acordados, mas também promover a adaptação às mudanças tecnológicas, regulamentares e às necessidades específicas da organização ao longo do tempo, garantindo a efetividade e a sustentabilidade da solução adotada.

3.25. **Os diferentes tipos de soluções em termos de especificação, composição ou caracterís ticas dos bens e serviços integrantes.**

3.25.1. Conforme levantamento de soluções analisadas no capítulo 6 “LEVANTAMENTO E ANÁLISE COMPARATIVA DE POSSÍVEIS CENÁRIOS”.

3.26. **A possibilidade de aquisição na forma de bens ou contratação como serviço.**

3.26.1. A solução objeto deste ETP será contratada no modelo de fornecimento como serviço (Software as a Service – SaaS), em conformidade com a

Instrução Normativa nº 5/2021 da GSI/PR e a Portaria nº 5950/2023 do Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

3.26.2. Esse modelo de contratação atende aos princípios da eficiência, escalabilidade e economicidade, permitindo que a administração pública utilize a solução de forma sob demanda, com atualizações contínuas, alta disponibilidade, e com infraestrutura sob responsabilidade do fornecedor. Além disso, o modelo SaaS favorece a aderência aos requisitos de segurança da informação, conforme estabelecido pela Estratégia de Governo Digital e pelas diretrizes da GSI/PR.

3.27. **A ampliação ou substituição da solução implantada.**

3.27.1. Não se aplica.

3.28. **As diferentes métricas de prestação do serviço e de pagamento.**

3.28.1. A modalidade de pagamento ocorrerá em consonância ao que fora postulado pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, as quais estarão definidas em nosso Termo de Referência correlato a esta contratação.

3.29. **RELAÇÃO ENTRE A DEMANDA PREVISTA E QUANTIDADE DE CADA ITEM**

3.29.1. A relação entre a demanda prevista e a quantidade foi prevista baseando-se nos cenários descritos nos itens de "Levantamento de Mercado" e de "Necessidade da Solução de TI", aos quais, após minuciosa análise concluiu-se os montantes expostos abaixo.

3.29.2. A tabela a seguir exibe o quantitativo obtido, para toda a arquitetura prevista, conforme nossa memória de cálculo apresentada para o consumo de Infraestrutura como Serviço e os demais serviços técnicos correlatos.

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	UN	580
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	UN	20
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	UN	41
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	UN	480
5	SERVIÇO DE INSTALAÇÃO	UN	4
6	TREINAMENTO POR PLATAFORMA	UN	4
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	UN	4

3.29.3. Todo o quantitativo estimado para contratação fora definido do tópico 3.3 “NECESSIDADES DA SOLUÇÃO DE TI – QUANTITATIVO ESTIMADO”.

3.30. **DEFINIÇÃO E ESPECIFICAÇÃO DE REQUISITOS**

3.30.1. Todas as quantidades, que definem o escopo global desta contratação, que visam atender ao Confea que requer o usufruto sob demanda da ferramenta de gestão de vulnerabilidades, estão detalhados no capítulo 3 “NECESSIDADE DA SOLUÇÃO DE TI”, deste Estudo Técnico Preliminar.

3.31. **NÍVEIS MÍNIMOS DE SERVIÇO (NMS)**

3.31.1. Toda a oferta deverá possuir, no mínimo, 36 (trinta e seis) meses de garantia e suporte técnico do(s) seu(s) respectivo(s) provedor(es), fabricante(s) e da CONTRATADA.

3.31.2. Os chamados de suporte técnico serão classificados por níveis de severidade de acordo como impacto no ambiente computacional da contratante, de acordo com as tabelas abaixo de Níveis de Severidade:

Nível	**Descrição do Impacto**
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos
3	Serviços disponíveis com ocorrência de alarmes de avisos
4	Dúvidas informacionais sobre as soluções vinculadas ao contrato

3.32. Prazos de Atendimento

Níveis de Severidade dos Chamados	Prazo	Níveis de Severidade			
Modalidade de Atendimento		1	2	3	4
Remoto	Início do Atendimento	1 hora	12 horas	24 horas	48 horas
Remoto	Solução de Contorno	8 horas	24horas	48 horas	72 horas

3.32.1. Entende-se por início de atendimento, o momento da abertura do chamado técnico.

3.32.2. Entende-se por término de atendimento a disponibilidade da solução implementada para uso em perfeitas condições de funcionamento no local onde está instalada.

3.32.3. O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado.

3.32.4. Nos casos específicos em que seja necessário o desenvolvimento de patches ou atualizações a nível de software, será admitida a execução das soluções de contorno até que seja desenvolvida uma nova versão de correção do problema.

3.32.5. Uma vez disponível, a CONTRATADA deverá auxiliar a CONTRATANTE com todo o processo de atualização seguro da solução.

3.32.6. O nível de severidade poderá ser reclassificado a critério da contratante. Caso isso ocorra, haverá o início de nova contagem de prazo, conforme o novo nível de severidade.

3.32.7. Depois de iniciado o atendimento, o mesmo não deverá ser interrompido até a recuperação do funcionamento dos serviços, salvo os casos em que a CONTRATANTE autorizar.

3.32.8. Quando um chamado não for solucionado no prazo máximo estabelecido, a equipe ou o técnico da Contratada deverá permanecer no atendimento até a completa solução do problema, sem ônus adicional para a Contratante, independentemente da aplicação de multas e penalidades contratuais.

3.32.9. Nestes casos deve ser respeitado o horário de expediente da Contratante, salvo se houver o acompanhamento e a ordem expressa da fiscalização do contrato para que os integrantes da Contratada permaneçam no local.

3.32.10. Quando houver um chamado aberto e pendente de solução que independa da Contratada, nos casos em que a atividade ensejar parada de serviço de rede ou no caso de existirem serviços essenciais que não possam ser paralisados, o trabalho poderá ser realizado após o horário estabelecido. Neste caso, a Contratada não será penalizada.

3.32.11. Todos os componentes de software deverão funcionar em conjunto, simultaneamente, sem conflitos, de forma integrada entre eles.

3.32.12. Os serviços deverão incorrer sob a mesma perspectiva de qualidade durante os 36 (trinta e seis) meses de garantia e contrato.

3.32.13. A execução dos serviços deve ocorrer conforme programação identificada nas Ordens de Serviço, que serão abertas quando demandado pelo Contratante à Contratada.

3.33. **ESTIMATIVAS PRELIMINARES DE PREÇO**

3.34. Com o intuito de subsidiar a pretensa contratação, foi efetuado o levantamento de contratações similares junto à Administração Pública, sendo analisados os Pregões realizados de maneira a auxiliar o Confea a obter a proposta mais vantajosa.

3.35. Conforme orienta a **Instrução Normativa Nº 65, de 07 de julho de 2021, Art. 5º** , a pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

> Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:
>
> I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;
>
> II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
>
> III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
>
> IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou
>
> V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

3.36. **Pesquisa de Preços e Metodologia, conforme tabelas abaixo:**

3.36.1. Para a composição estatística, a qual define o valor estimado desta contratação, o Confea *executou 2 (dois) tipos de pesquisas distintas* , sendo uma pautada nos processos públicos e outra na coleta de propostas de distintos fornecedores.

3.36.2. Quanto a aferição de possíveis referências de preços para esta contratação, inicialmente, foram averiguados processos públicos na federação com o intuito de identificar escopos similares para atender a necessidade do Confea. Detalhamos a seguir alguns processos identificados e seus contextos.

3.36.3. Contabilizaremos na memória de cálculo somente aqueles processos que forem aderentes ao nosso escopo e puderem, de modo equitativo, serem devidamente comparados a nossa demanda para computarmos seus custos com a nossa contratação.

3.37. **PESQUISA DE PREÇOS PÚBLICOS**

3.37.1. Para a formação do orçamento desta contratação foram considerados os quantitativos apresentados na seção anterior deste Estudo Técnico Preliminar;

3.37.2. Diante de fatores macroeconômicos como a flutuação do dólar e outras variáveis imprevisíveis, torna-se imprescindível a realização de uma pesquisa de mercado para assegurar a melhor decisão de investimento;

3.37.3. De antemão, ressaltamos que apesar de existirem preços públicos de alguns itens similares a nossa contratação, **nem todo o escopo pretendido fora identificado** em projetos passados dentro da federação, nem fora identificado processo recente, com prazo de validade condizente com a pesquisa feita (até um ano da homologação);

3.37.4. Nesse sentido, com o intuito de não confeccionarmos uma referência errônea quanto ao mapa de preços do projeto, o CONFEA optou pela coleta de propostas comerciais conforme as condições estabelecidas na legislação vigente e com base na Lei Federal n° 14.133/2021, em consonância ao que preconiza o Governo Federal:

> *Art. 23. O valor previamente estimado da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.*
>
> *§ 1º No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com base no melhor preço aferido por meio da utilização dos seguintes parâmetros, adotados de forma combinada ou não:*
>
> *I - composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde disponíveis no Portal Nacional de Contratações Públicas (PNCP);*
>
> *II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;*
>
> *III - utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que contenham a data e hora de acesso;*
>
> *IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;*

ID	ÓRGÃO (Pregão Eletrônico – UASG)	OBJETO	VALOR DA CONTRATAÇÃO	DATA DE HOMOLOGAÇÃO
1	Tribunal de contas da União DF (2024 – 90015 / 30001)	Fornecimento de direito de uso de licenças de software como serviço da solução de gerenciamento de vulnerabilidades Qualys Vulnerability Management, Detection and Response (VMDR)	R$ 248.832,00	27/08/2024
2	DETRAN-RO (926002/2024 – 90053)	Aquisição das Licenças da Solução de Gestão de Vulnerabilidades RAPID7 para atender a Coordenadoria de Tecnologia da Informação/CTI deste DETRAN/RO, conforme especificações estabelecidas no Termo de Referência (0048911087).	R$ 1.685.300,00	20/08/2024
3	TRIBUNAL DE JUSTIÇA DO ESTADO DE RONDÔNIA (925006/2024 –90010)	Registro de preços para eventual fornecimento de licenças da Plataforma de Gerenciamento de Exposição Tenable One, para atualização (upgrade) da versão Tenable Nessus, para atender o Tribunal de Justiça do Estado de Rondônia, conforme as disposições deste Edital e seus Anexos	R$ 2.223.800,00	17/12/2024

3.37.5. A pesquisa considerou valores praticados para soluções de proteção e gestão de vulnerabilidades, levando em conta o escopo funcional, os requisitos técnicos mínimos e a quantidade estimada de ativos a serem atendidos.

3.37.6. Entretanto, verificou-se que os preços obtidos durante a pesquisa não são compatíveis com as necessidades específicas do CONFEA, especialmente sob a ótica de funcionalidades.

3.37.7. Os fornecedores consultados apresentaram propostas dimensionadas para volumes de ativos voltados a gestão de vulnerabilidades, porém não com todo o ferramental exigido pelo CONFEA, como gestão de superfície de ataque e gestão de vulnerabilidades para Active Directory.

3.37.8. Ademais, explicitamos a análise do CONFEA referente aos valores identificados.

3.38. **PROCESSO DE ID 01, preços identificados:**

NECESSIDADE DO CONFEA		PROCESSO 01		
Item	Descrição	Item	Descrição	Valor Unitário

1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	1	Licença Qualys Vulnerability Management Detection and Response (VMDR)	R$ 364,50 (valor unitário multiplicado por 3)
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
5	SERVIÇO DE INSTALAÇÃO	N/A	N/A	N/A
6	TREINAMENTO POR PLATAFORMA	N/A	N/A	N/A
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	N/A	N/A	N/A

3.38.1. Nesse sentido, fica explícito que o processo em voga carece dos demais elementos necessários a contratação do CONFEA.

3.39. **PROCESSO DE ID 02, preços identificados:**

NECESSIDADE DO CONFEA		PROCESSO 02		
Item	Descrição	Item	Descrição	Valor Unitário
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	1	Garantia e Suporte Técnico 24 x 7 da Solução (InsightVM Subscription Rapid7 SKU IVM / PTERMS da RAPID7) – com direito a atualização de novas versões do fabricante e vigência de 60 (sessenta) meses.	R$ 532,20 (valor unitário dividido por 5 e multiplicado por 3)
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
5	SERVIÇO DE INSTALAÇÃO	N/A	N/A	N/A
6	TREINAMENTO POR PLATAFORMA	N/A	N/A	N/A
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	N/A	N/A	N/A

3.39.1. Nesse sentido, fica explícito que o processo em voga carece dos demais elementos necessários a contratação do CONFEA.

3.39.2. **PROCESSO DE ID 03, preços identificados:**

NECESSIDADE DO CONFEA		PROCESSO 03		
Item	Descrição	Item	Descrição	Valor Unitário
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	1	Subscrição do licenciamento do software de gestão de vulnerabilidades Tenable One, para atualização (upgrade) da versão Tenable Nessus Professional atualmente em uso	R$ 1.086,00 (valor unitário dividido multiplicado por 3)
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	N/A	N/A	N/A
5	SERVIÇO DE INSTALAÇÃO	N/A	N/A	N/A
6	TREINAMENTO POR PLATAFORMA	1	Treinamento e Capacitação para até 15 usuários	27.200,00 (valor unitário dividido por 15 e multiplicado por 4)
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	2	Serviço de Suporte Técnico Especializado com Operação Assistida	392.400,00 (valor unitário multiplicado por 3)

3.39.3. Nesse sentido, fica explícito que o processo em voga carece dos demais elementos necessários a contratação do CONFEA.

ITEM	VALORES UNITÁRIOS			MEDIANA*	DESVIO PADRÃO	INEXEQUÍVEIS (MEDIANA - DESVIO PADRÃO)	ELEVADOS (MEDIANA + DESVIO PADRÃO)
	PROCESSO 01	PROCESSO 02	PROCESSO 03				
1	364,50	532,20	1.086,00	532,20	308,29	223,91	840,49
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	27.200,00	-	12.822,20	12.822,20	12.822,20

7	-	-	392.400,00	-	184.979,13	-	184.979,13	184.979,13

3.40. *A Mediana representa o ponto central entre as amostras.

3.40.1. A soma e a subtração da mediana em relação ao desvio padrão (de todas as amostras), nos permite apurar valores inexequíveis ou elevados.

3.40.2. Os valores considerados na segunda etapa da memória de cálculo serão aqueles que estiverem dentro do intervalo exequível de cada item.

3.40.3. A pesquisa carece de amostras suficientes para a apuração correta do valor estimado da contratação.

3.40.4. Diante das pesquisas feitas, a não existência de um escopo integral de atendimento para a gestão de vulnerabilidades do ambiente completo do CONFEA e a variação elevada entre os preços de distintas fabricantes, os valores para a formação da correta memória de cálculo deverão ser complementados por propostas de fornecedores.

3.41. **MAPA COMPARATIVO DO CUSTO TOTAL DE PROPRIEDADE (TCO)**

3.41.1. Para a formação do orçamento desta contratação foram considerados os quantitativos apresentados na seção anterior deste Estudo Técnico Preliminar;

3.41.2. Diante de fatores macroeconômicos como a flutuação do dólar e outras variáveis imprevisíveis, torna-se imprescindível a realização de uma pesquisa de mercado para assegurar a melhor decisão de investimento;

3.41.3. Nesse sentido, com o intuito de não confeccionarmos uma referência errônea quanto ao mapa de preços do projeto, o CONFEA optou pela coleta de propostas comerciais conforme as condições estabelecidas na legislação vigente e com base na Lei Federal n° 14.133/2021, em consonância ao que preconiza o Governo Federal:

> *Art. 23. O valor previamente estimado da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.*
>
> *§ 1º No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com base no melhor preço aferido por meio da utilização dos seguintes parâmetros, adotados de forma combinada ou não:*
>
> *I - composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde disponíveis no Portal Nacional de Contratações Públicas (PNCP);*
>
> *II - Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;*
>
> *III - Utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que contenham a data e hora de acesso;*
>
> *IV - Pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;*

3.42. Destacamos a seguir as propostas comerciais coletadas para a estimativa dos custos desta contratação:

3.43. **PROPOSTA 01**

3.43.1. VALIDADE: 120 (cento e vinte) dias consecutivos

3.43.2. TABELA DE ITENS:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	UNITÁRIO (R$)	TOTAL (R$)
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	UN	580	R$ 1.844,05	R$ 1.069.548,46
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	UN	20	R$ 1.647,16	R$ 32.943,28
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	UN	41	R$ 874,73	R$ 35.863,84
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	UN	480	R$ 884,08	R$ 424.357,27
5	SERVIÇO DE INSTALAÇÃO	UN	4	R$ 54.481,79	R$ 217.927,17
6	TREINAMENTO POR PLATAFORMA	UN	4	R$ 26.331,64	R$ 105.326,57
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	UN	4	R$ 66.917,27	R$ 267.669,08
TOTAL					R$ 2.153.635,67

3.44. **PROPOSTA 02**

3.44.1. VALIDADE: 120 (cento e vinte) dias

3.44.2. TABELA DE ITENS:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	UNITÁRIO (R$)	TOTAL (R$)
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	UN	580	R$ 2.477,75	R$ 1.437.095,00
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	UN	20	R$ 2.390,83	R$ 47.816,60
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	UN	41	R$ 2.380,95	R$ 97.61,95
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	UN	480	R$ 2.381,60	R$ 1.143.168,00
5	SERVIÇO DE INSTALAÇÃO	UN	4	R$ 49.571,63	R$ 198.286,52
6	TREINAMENTO POR PLATAFORMA	UN	4	R$ 34.702,09	R$ 138.808,36
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	UN	4	R$ 65.201,68	R$ 260.806,72
TOTAL					R$ 3.323.600,15

3.45. **PROPOSTA 03**

3.45.1. VALIDADE: 90 (noventa) dias

3.45.2. TABELA DE ITENS:

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	UNITARIO (R$)	TOTAL (R$)
1	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA	UN	580	R$ 2.072,34	R$ 1.201.955,21
2	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB, COM 36 MESES DE VIGÊNCIA	UN	20	R$ 1.859,88	R$ 37.197,59
3	LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE, COM 36 MESES DE VIGÊNCIA	UN	41	R$ 968,63	R$ 39.713,90
4	LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY, COM 36 MESES DE VIGÊNCIA	UN	480	R$ 994,26	R$ 477.246,69
5	SERVIÇO DE INSTALAÇÃO	UN	4	R$ 61.895,67	R$ 247.582,67
6	TREINAMENTO POR PLATAFORMA	UN	4	R$ 29.939,53	R$ 119.758,11
7	SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES	UN	4	R$ 75.054,44	R$ 300.217,77
TOTAL					R$ 2.423.671,95

3.46. **JUSTIFICATIVA DA SOLUÇÃO/NEGÓCIO**

3.46.1. O A administração pública depende, cada vez mais, de sistemas informatizados para a execução de suas atividades essenciais e para a oferta de serviços à sociedade. Neste cenário, a segurança da informação torna-se um pilar estratégico para garantir a continuidade dos serviços, a integridade dos dados públicos e a confiança dos cidadãos. A crescente sofisticação das ameaças cibernéticas e o aumento da superfície de ataque exigem medidas proativas de proteção dos ativos tecnológicos do governo.

3.46.2. A ausência de uma ferramenta de gestão de vulnerabilidades limita a capacidade do órgão em identificar e tratar, de forma eficaz, falhas de segurança nos sistemas, dispositivos e aplicações sob sua responsabilidade. A abordagem manual ou reativa compromete a visibilidade sobre os riscos reais, aumenta o tempo de exposição a ameaças conhecidas e dificulta o tratamento adequado das vulnerabilidades detectadas. Isso pode resultar em incidentes com impactos significativos sobre a imagem institucional, os serviços públicos e os dados sensíveis da população.

3.46.3. A aquisição de uma ferramenta especializada permitirá automatizar a identificação e análise de vulnerabilidades em todo o ambiente tecnológico, promovendo uma visão centralizada e contínua dos riscos. Com recursos de priorização baseada em criticidade, contexto do ativo e probabilidade de exploração, será possível direcionar os esforços de correção de forma mais eficiente, conforme os princípios de economicidade e eficácia da gestão pública.

3.46.4. Além disso, a adoção dessa solução atenderá a exigências legais e normativas, como as diretrizes da Estratégia Nacional de Segurança Cibernética (E-Ciber), o Decreto nº 10.748/2021 (que institui a Política Nacional de Segurança da Informação), e os controles previstos no Guia de Gestão de Riscos da CGU, bem como em normas técnicas reconhecidas, como a ISO/IEC 27001 e o NIST SP 800-53. Também contribuirá para o cumprimento dos requisitos de governança estabelecidos pelos órgãos de controle e para a melhoria contínua dos processos de segurança da informação.

3.46.5. Dessa forma, justifica-se a necessidade de contratação de uma ferramenta de gestão de vulnerabilidades como parte integrante da estratégia institucional de cibersegurança. Trata-se de um investimento essencial para fortalecer a resiliência digital do órgão, proteger informações críticas e assegurar a prestação segura, eficiente e ininterrupta dos serviços públicos à população.

3.47. **JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO**

3.47.1. O agrupamento dos itens do objeto do presente Instrumento em lote único, tem por objetivo a padronização da contratação uma vez que os itens agrupados possuem a mesma natureza técnica, especificadas para o contexto de Segurança como serviço (SaaS), o que resulta ainda na otimização de recursos tecnológicos, humanos e financeiros, facilitando o desenvolvimento das atividades relacionadas à gestão contratual.

3.47.2. O gerenciamento de um número variado de fornecedores traz consigo a ineficiência e a complexidade da gestão e da fiscalização do contrato. Em razão da pluralidade das soluções e seu parcelamento em lotes correlatos torna o contrato técnica, econômica e administrativamente inviável ou ainda provoca a perda de economia de escala.

3.47.3. Neste sentido, justifica-se o agrupamento em lote por natureza técnica, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficácia, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

3.47.4. Logo, as vantagens seriam o maior nível de controle pela Administração quanto a execução da prestação dos serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos e na mensuração da qualidade de serviço e a concentração da responsabilidade pela execução a cargo de um único fornecedor. Tais aspectos facilitam assim o acompanhamento dos resultados, para o objeto estabelecido na contratação.

3.47.5. Os serviços que constituem o objeto enquadram-se no conceito de serviços comuns onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida e ainda se averiguou que os distintos itens destacados no lote são comercializados por múltiplas empresas no mercado nacional, das quais disponibilizam ofertas integrais de distintos provedores de serviços de infraestrutura internacionais.

3.47.6. Os Itens do Lote tratam da composição de solução de Gestão de Vulnerabilidades, de serviço de instalação, de serviço continuado e de serviço de treinamento todos eles correlatos entre si, integralmente, formatando assim uma solução tecnológica completa, orientada a realidade atual e futura do CONFEA.

3.47.7. Requisitamos, dentro dessa contratação, que todos os elementos presentes façam parte de uma solução integrada e interoperável, de modo a permitir que o fluxo de informações presentes seja seguro e possua versionamento suficiente para mitigarmos eventos de desastres que possam vir a ocorrer.

3.47.8. É de nosso entendimento que todos os elementos presentes participarão de um design lógico voltado a dirimir as vulnerabilidades do ambiente de TI, a segurança do acesso e a segurança contínua dos dados, onde apesar da atuação micro, de cada componente ao seu escopo específico, todos os elementos fomentarão uma estratégia de produção e contingenciamento digital.

3.47.9. Assim, cabe esclarecer também que a correta e completa implantação é parte fundamental para a execução desse projeto. Os serviços correlatos a essa contratação exigem que a CONTRATADA tenha qualidade técnica suficiente para mantermos a longevidade da aquisição, alinhando nossas expectativas com os objetivos estratégicos.

3.47.10. Portanto, consideramos os itens do lote como correlacionados entre si, de modo que eles formam uma solução integrada, devendo serem licitados em um grupo e entregues por tão somente uma empresa. O principal intuito tange a garantia de que apenas uma entrega minimiza o risco de fornecimento parcial da solução, ou ainda o risco de compartilhamento de responsabilidades entre diferentes fornecedores, o que comprometeria os resultados dos projetos.

3.47.11. Pelo exposto, não há restrição da competitividade ao adquirir todos os itens de um mesmo fornecedor, já que é prática comum do mercado a realização da venda, da instalação e da configuração por uma única CONTRATADA, do seu lote específico.

3.47.12. **PROVA DE CONCEITO E TESTE DE CONFORMIDADE**

3.47.13. Não será exigida prova de conceito, nem teste de conformidade para esta contratação.

3.47.14. O rol de pré-requisitos para a apresentação de propostas técnicas e comerciais serão suficientes para avaliar tecnicamente a capacidade da proponente participante do processo.

3.48. **CRONOGRAMA DE EXECUÇAO**

3.48.1. O cronograma de execução será elaborado e aprovado pela Contratante, podendo, após assinatura do contrato, sofrer alterações conforme os prazos estabelecidos.

3.48.2. O cronograma de execução será executado conforme os prazos estabelecidos entre a contratada e o Confea.

3.48.3. As datas poderão sofrer alterações em comum acordo entre o Contratante e a Contratada, desde que não prejudiquem o andamento e a entrega dos serviços no prazo estabelecido.

3.48.4. O atraso no cumprimento das etapas do cronograma ensejará multa conforme estabelecerá o edital de licitação relacionado ao Termo de Referência.

Etapa	Descrição	Quando Ocorre	Prazos Estimados (Dias Corridos)	
			Início	Término
1	Assinatura do Contrato	Em até 10 (dez) dias após a assinatura do Contrato	0	10
2	Reunião presencial de alinhamento de expectativas	Em até 10 (dez) dias após a reunião de alinhamento de expectativas	11	21
3	Emissão da Ordem de Serviço	Em até 10 (dez) dias após a reunião de alinhamento de expectativas	22	32
4	Liberação da licença ou de acesso a plataforma	Em até 20 (vinte) dias, contados a partir da emissão da Ordem de Serviço	33	53
5	Projeto de Implantação	Em até 30 dias da reunião presencial de alinhamento de expectativas	54	84
6	Treinamento	Em até 60 dias da reunião presencial de alinhamento de expectativas	85	145
7	Implantação	Em até 30 dias após a entrega do projeto de implantação	146	176
8	Recebimento provisório	Mediante termo de recebimento provisório após efetuada a entrega dos serviços para posterior verificação de sua conformidade com as especificações	177	187
9	Recebimento definitivo	Mediante termo de recebimento definitivo em até 10 (dez) dias úteis após o recebimento provisório e a verificação da perfeita execução das obrigações contratuais	188	198
10	Início do período de execução do serviço	A partir do termo de recebimento definitivo dos serviços	199	12 meses*
11	Pagamento relativo ao serviço contratado	Até 15 (dez) dias úteis após o recebimento definitivo, se não houver impedimentos	-	-

3.48.5. Todo o cronograma de serviços deverá ser executado mediante a apresentação do volume de serviços necessários a contratação, para a execução do projeto, conforme demonstrado em nosso catálogo de serviços já estimado neste Estudo Técnico.

3.48.6. O pagamento dos serviços ocorrerá sob demanda, conforme os itens contratados e em consonância as suas métricas individuais de consumo.

3.49. **NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL**

3.49.1. **TECNOLÓGICA:** Não há necessidade de investimento adicional em infraestrutura.

3.49.2. **REDE ELÉTRICA:** Não há necessidade de adequação do ambiente.

3.49.3. **LOGÍSTICA:** Não há necessidade de adequação.

3.49.4. **MOBILIÁRIO:** Não há necessidade de adequação do ambiente.

3.49.5. **OUTRAS ADEQUAÇÕES:** Não há necessidade de adequação do ambiente.

3.50. **RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO**

3.50.1. Recursos materiais e humanos

3.50.2. A Equipe de Fiscalização da Contratação a ser constituída que será a responsável pelo acionamento da empresa e acompanhamento das tarefas realizadas por seus técnicos, bem como pelas atividades relacionadas à fiscalização do contrato.

3.50.3. Não serão necessários recursos materiais e humanos adicionais para a contratação almejada, porém, os recursos humanos necessários para viabilizar a execução contratual serão do quadro de empregados do Confea, conforme abaixo evidenciado.

Id	Função	Formação	Atribuição
1	Fiscal Técnico do Contrato	Empregado representante da Área de TI	Fiscalizar os aspectos técnicos do contrato
2	Fiscal Requisitante do Contrato	Empregado representante da Área Requisitante da solução	Fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TI
3	Fiscal Administrativo do Contrato	Empregado representante da Área Administrativa	Fiscalizar o contrato quanto aos aspectos administrativos
4	Gestor do contrato	Empregado do Confea com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato	Coordenar e comandar o processo de gestão e fiscalização da execução contratual
5	Preposto da Empresa Contratada	Empregado da empresa contratada que atua em nome da empresa na área correlata à execução contratual	Representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual

3.51. **ESTRATÉGIA DE CONTINUIDADE CONTRATUAL**

3.51.1. Para assegurar a continuidade da solução, acionar-se-ão as seguintes ações para os eventos apresentados na tabela abaixo em complemento à "Identificação e Gerenciamento de Riscos", tratado em tópico específico neste Estudo Técnico Preliminar.

ID	Evento	Ação Preventiva	Responsáveis	Ação de Contingência	Responsáveis

1	Falência/Inexistência da empresa	Exigência de documentação que comprove a saúde financeira da empresa, bem como caução/seguro referente ao valor do contrato	Gerência de Contratações e Equipe de Planejamento do Contratação	Convocação da próxima colocada no certame, se ainda possível. Repasse das atribuições da empresa anteriormente contratada, caso tenha conhecimento inerente e de forma comprovada. Auxílio das equipes internas do Confea, no que couber, e de acordo com cada especialidade	Equipe de Fiscalização do Contrato e Gestor do Contrato
2	Inexecução do contrato	Exercer os papeis fiscalizatórios perante a contratada de modo a acompanhar a execução contratual	Equipe de Fiscalização do Contrato	Manter a execução do contrato para as demandas mais urgentes, realizar novo planejamento da contratação e realizar rescisão do contrato vigente dada a inexecução	Equipe de Fiscalização do Contrato e Gestor do Contrato
3	Encerramento da vigência do contrato, sem possibilidade de prorrogação	Avaliar as cláusulas contratuais e comunicar à gestão a necessidade de condução de novo processo licitatório	Gerente de Tecnologia da Informação	Realizar novo processo de planejamento e contratação de serviços	Equipe de Planejamento da Contratação
4	Encerramento da vigência do contrato, com possibilidade de prorrogação	Avaliar as cláusulas contratuais e comunicar à gestão a necessidade de aditivo ao contrato	Equipe de Fiscalização do Contrato e Gerente de Tecnologia da Informação	Verificar a manutenção da necessidade, economicidade e oportunidade da contratação e realizar o aditamento contratual, se houver a prorrogação	Gerente de Tecnologia da Informação e Gerência de Contratações
5	Capacitação na operação do objeto/serviço	Previsão contratual de capacitação (transferência de conhecimento) da solução adquirida	Equipe de Planejamento da Contratação	Contratação de manutenção e suporte	Equipe de Fiscalização do Contrato e Gestor do Contrato

3.52. **IDENTIFICAÇÃO E GERENCIAMENTO DE RISCOS**

3.52.1. Cumprindo com o disposto no art. 38 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, foram analisados os riscos inerentes a três situações distintas relacionadas a este processo de contratação, que são as fases de Planejamento da Contratação, Seleção do Fornecedor e Contratação da Solução.

3.52.2. Consoante doc. (1376225) - Análise de Riscos de TIC.

3.53. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

3.53.1. Conforme dispõe a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, em seu artigo 11, inciso V: Art. 11. O Estudo Técnico Preliminar da Contratação será realizado pelos Integrantes Técnico e Requisitante, compreendendo, no mínimo, as seguintes tarefas: V - declaração da viabilidade da contratação, contendo a justificativa da solução escolhida, que deverá abranger a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

3.53.2. Esta Equipe de Planejamento da Contratação entende ser VIÁVEL a contratação da solução demandada, levando-se em consideração toda a justificativa já efetuada, incluindo os benefícios de sua adoção, contida nos itens "Necessidade da Solução de TI" e "Justificativa da Solução Escolhida" deste Estudo Técnico Preliminar.

3.53.3. Ainda, objetiva-se como benefícios, dentre outros:

3.53.4. A disponibilização de recursos universais, que estendem o escopo do Confea e atendem, simultaneamente, os mais plurais Conselhos Regionais de Engenharia e Arquitetura espalhados geograficamente na federação.

3.53.5. Com a contratação em voga, pretendemos garantir o usufruto da tecnologia em prol do serviço público, sem a necessidade de investimento em soluções complexas de TIC, as quais passam por longos processos de análise de viabilidade ao longo de seus ciclos de vida.

3.53.6. Em cumprimento ao disposto no art. 11, parágrafos segundo e terceiro, da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, "o Estudo Técnico Preliminar da Contratação será aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC", bem como, "caso a autoridade máxima da Área de TIC venha a compor a Equipe de Planejamento da Contratação, a autoridade que assinará o Estudo Técnico Preliminar da Contratação será aquela superior à autoridade máxima da Área de TIC".

3.53.7. Dessa forma, o presente documento segue assinado pelos Integrantes Requisitante e Técnico da Equipe de Planejamento da Contratação designados pelo documento de Instituição da Equipe de Planejamento da Contratação na Portaria nº 273/2024 (doc. 0981866), bem como por seus gestores superiores.

Documento assinado eletronicamente por **Vinicius de Assis Lima**, **Integrante Requisitante**, em 23/02/2026, às 11:15, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo de Oliveira Coelho Santos**, **Integrante Técnico**, em 23/02/2026, às 11:22, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alberto de Azevedo Santos**, **Integrante Administrativo**, em 23/02/2026, às 11:24, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Pedro Kiyoshi Nakano**, **Gerente de Inovação e Transformação**, em 23/02/2026, às 11:34, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://confea.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1478206** e o código CRC **0C058AE3**.

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

INFORMAÇÃO CONFEA-GSI Nº 10/2026

Processo: 00.003608/2024-71
Tipo de Processo: Aquisição/Contratação: Bens ou Serviços
Assunto: Fornecimento de Software/Serviço de Gestão de Vulnerabilidades
Interessado: Setor de Infraestrutura e Arquitetura

ANEXO I – ESPECIFICAÇÕES TÉCNICAS
QUADRO RESUMO DA CONTRATAÇÃO

LOTE ÚNICO				
ITEM	**CATSER**	**DESCRIÇÃO**	**UNIDADE**	**QTD TOTAL**
1	27464	Licenciamento para a Gestão de Vulnerabilidades	UN	11080
2	27464	Licenciamento para a Gestão de Vulnerabilidades de *Aplicações Web*	UN	230
3	27464	Licenciamento para a Gestão de Superfície de Ataque	UN	781
4	27464	Licenciamento para a Gestão de Vulnerabilidades para *Active Directory*	UN	26380
5	26972	Serviço de Instalação	UN	16
6	3840	Treinamento por Plataforma	UN	16
7	27014	Serviço Continuado para a Gestão de Vulnerabilidades	UN	144

1. CARACTERÍSTICAS GERAIS DA CONTRATAÇÃO

1.1. A presente contratação tem por objeto a aquisição de uma ferramenta de gestão de vulnerabilidades com o objetivo de fortalecer a segurança da informação no âmbito do CONTRATANTE, por meio da identificação contínua, análise, priorização e tratamento de vulnerabilidades em ativos tecnológicos.

1.1.1. A solução deverá contemplar funcionalidades integradas que permitam a execução automatizada de varreduras em redes, servidores, aplicações e demais dispositivos, bem como a geração de relatórios gerenciais e técnicos que subsidiem a tomada de decisões estratégicas pela área de Tecnologia da Informação.

1.2. A ferramenta contratada deverá ser entregue pronta para uso (*turn-key*), devendo incluir todos os módulos e componentes necessários para seu pleno funcionamento, inclusive funcionalidades de correlação de riscos, priorização com base em critérios e integração com bases públicas de dados de ameaças (como NIST/NVD).

1.2.1. A solução deverá ser disponibilizada em um dos seguintes modelos: SaaS (Software como Serviço), hospedada em nuvem, ou instalada em ambiente *on-premises*.

1.2.2. Caso a oferta compreenda uma solução fornecida da modalidade SaaS, ela obrigatoriamente deverá atender a exigência do Art. 18 da IN 05/2021, a qual menciona:

> Art. 18. Os dados, *metadados*, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:
>
> I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

1.3. A ferramenta deverá permitir a gestão centralizada das vulnerabilidades, com a visualização de painéis (*dashboards*) customizáveis, emissão de alertas automáticos, geração de indicadores de desempenho e possibilidade de integração com sistemas de terceiros por meio de APIs.

1.3.1. É fundamental que a solução atenda aos princípios de segurança, escalabilidade, disponibilidade e interoperabilidade, alinhando-se às boas práticas e normativos nacionais e internacionais, como a ISO/IEC

27001, ISO/IEC 27002, LGPD e as orientações do TCU e da Estratégia Nacional de Segurança Cibernética (E-Ciber).

1.4. A solução deverá operar com baixa intervenção manual, permitindo o agendamento automático de varreduras periódicas e a correlação inteligente entre vulnerabilidades detectadas e ameaças conhecidas, facilitando o trabalho da equipe de segurança da informação. Também deverá possuir mecanismos de controle de acesso baseado em perfis (RBAC), registro de auditoria e rastreabilidade das ações realizadas pelos usuários.

1.5. Em resumo, a contratação visa dotar o CONTRATANTE de uma solução tecnológica robusta e eficiente, que possibilite visibilidade ampla e em tempo real do cenário de riscos de segurança cibernética, contribuindo diretamente para a proteção dos sistemas institucionais, a conformidade legal e regulatória, e a continuidade dos serviços públicos digitais oferecidos à sociedade.

2. REQUISITOS DE INSTALAÇÃO DAS SOLUÇÕES

2.1. Independentemente do volume de licenças adquiridas pelo CONTRATANTE , será de responsabilidade da CONTRATADA, após o fornecimento de qualquer um dos licenciamentos previstos, executar todos os procedimentos de instalação para a correta operacionalização da solução.

2.2. Será de responsabilidade da CONTRATADA:

2.2.1. Apoiar a CONTRATANTE na definição da arquitetura da solução, a qual deverá incluir a topologia, os pontos de análise e a aplicação de regras iniciais para a gestão de vulnerabilidades.

2.2.2. Aplicar todas as licenças e patches de atualização, seja na solução ou em componentes dela a depender de sua arquitetura.

2.2.3. Executar todas as configurações para o gerenciamento remoto da solução, incluindo a configuração de usuário administrador e todos os serviços de rede essenciais ao seu funcionamento.

2.2.4. Implantar a solução conforme as boas práticas da fabricante, incluindo todas as ações mínimas para a execução de, ao menos, 3 (três) varreduras por vulnerabilidades no ambiente.

2.3. Após o término dos procedimentos de configuração, a CONTRATADA deverá:

2.3.1. Executar os testes de validação de varredura e observar o comportamento adequado da solução.

2.3.2. Executar os testes para a homologação do projeto, incluindo a estabilidade da solução e a correta varredura dos mais distintos contextos previstos.

2.4. A CONTRATADA deverá emitir relatório *As-Built* de todos os procedimentos executados, incluindo diagramas lógicos e físicos (quando couber).

3. ITEM 1 – LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES, COM 36 MESES DE VIGÊNCIA

3.1. **Características gerais:**

3.1.1. Cada unidade de *software* contratada, deverá corresponder a gestão de vulnerabilidade de 1 (um) ativo de rede da CONTRATANTE.

3.1.2. O software deverá ser fornecido na modalidade de subscrição e deverá possuir garantia oficial da fabricante da oferta pelo período de 36 (trinta e seis) meses.

3.1.3. As licenças deverão estar no nome do CONTRATANTE, não serão aceitas licenças utilizadas na prestação de serviços;

3.1.4. A solução deve realizar varreduras (*scans*) de vulnerabilidades, avaliação de configuração e conformidade (*baseline e compliance*);

3.1.5. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

3.1.6. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

3.1.7. A solução deve ser licenciada pelo número de endereços IP ou dispositivos (*assets*);

3.1.8. A solução deve fornecer um modelo de armazenamento integrado que não dependa de um banco de dados externos ou de terceiros;

3.1.8.1. Caso a solução dependa de banco de dados de terceiros, todas as licenças deverão ser fornecidas pela CONTRATADA.

3.1.9. A solução deverá suportar API (Application Programming Interface) baseada em REST (Representatonal State Transfer) para automação de processos e integração com aplicações terceiras.

3.1.10. A solução deve possuir integração via API no mínimo as seguintes linguagens: *Python, Powershell, Ruby, javascript, Java, Swift e PHP*;

3.1.11. A solução deve possuir métodos de consulta via API e envio, tais como: HTTP METHOD (POST, GET, PUT AND DELETE);

3.1.12. A solução deve incluir a opção para agentes instalados e licenciados em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

3.1.12.1. Tais agentes devem ser gerenciados pela mesma interface/console da plataforma de gestão de vulnerabilidades;

3.1.13. A solução deve permitir o agrupamento de *scanners* para facilitar o gerenciamento e aplicação de políticas;

3.1.14. A solução deve realizar a varredura tanto de dispositivos na rede interna, dispositivos expostos a demais redes externas, tanto quanto dispositivos em nuvens públicas como Azure, AWS ou GCP;

3.1.15. O escaneamento para os dispositivos expostos deve sem realizados através de *SCANS* (ENGINE) do próprio fabricante alocados no Brasil;

3.1.16. Os *scanners* e sensores agentes deverão ser gerenciados por uma única plataforma, de maneira centralizada;

3.1.17. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

3.1.18. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

3.1.19. A solução deve apresentar, para cada vulnerabilidade encontrada, a descrição e passos que devem ser tomados para correção;

3.1.20. A solução deve apresentar, para cada vulnerabilidade encontrada, evidências da vulnerabilidade através de saídas das verificações (outputs);

3.1.21. A solução deve fornecer controle de acesso baseado em função (RBAC- Role Based Access Control) para controlar o acesso do usuário a conjuntos de dados e funcionalidades;

3.1.22. A solução deve ser capaz de definir e gerenciar grupos de usuários, incluindo limitação de funções de varreduras e acesso a relatórios e dashboards;

3.1.23. A solução deve ter a capacidade de excluir determinados endereços IP do escopo de qualquer varredura ou scan;

3.1.24. A solução deve criptografar todos resultados de varreduras obtidos e informações inseridas tanto em descanso quanto em trânsito;

3.1.25. A solução deve suportar métodos de autenticação usando bases de autenticação local, e SAML (Security Assertion Markup Language) para uso de SSO (Single Sign-On);

3.1.26. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

3.1.27. A solução não deve impor nenhum limite de quantidade de scanners implementados dentro da infraestrutura;

3.1.28. A solução deverá possuir sistema de alertas para informar a disponibilidade de resultados dos escaneamentos através de email;

3.1.29. A solução deve oferecer capacidade de configuração dinâmica de grupos de ativos através de no mínimo as seguintes características:

3.1.29.1. Sistema Operacional, Endereço IP, DNS, NetBIOS Host, MAC, AWS Instance Type, AWS EC2 Name, Software instalado, Azure VM ID, AWS Region, Google Cloud Instance ID, Azure Resource ID, Ativos avaliados;

3.2. Dos requisitos e relatórios e painéis gerenciais

3.2.1. A solução deverá possuir painéis gerenciais (dashboards) pré-definidos para rápida visualização dos resultados, permitindo ainda a criação de painéis personalizados;

3.2.2. Os painéis gerenciais deverão ser apresentados em diversos formatos, incluindo gráficos e tabelas, possibilitando a exibição de informações em diferentes níveis de detalhamento;

3.2.3. Os relatórios devem ser disponibilizados sob demanda no console de gerência da solução;

3.2.4. Os relatórios devem conter informações da vulnerabilidade, severidade, se existe um exploit disponível e informações do ativo;

3.2.5. A solução deve permitir a customização de dashboards/relatórios;

3.2.6. A solução deve concentrar todos os relatórios na plataforma central de gerenciamento, não sendo

aceitas soluções fragmentadas;

3.2.7. A solução deve ser capaz de produzir relatórios, pelo menos, nos seguintes formatos: HTML, PDF e CSV;

3.2.8. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

3.2.9. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

3.2.10. A solução deve suportar o envio automático de relatórios para destinatários específicos;

3.2.11. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

3.2.12. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

3.3. Das varreduras

3.3.1. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como appliances virtuais;

3.3.2. A solução deve suportar varredura com e sem agente, de maneira ativa e passiva, distribuídas em diferentes localidades e regiões e gerenciar todos por uma console central;

3.3.3. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de vulnerabilidades;

3.3.4. Tais agentes devem realizar conexões para o sistema gerenciamento através de protocolo seguro;

3.3.5. A solução deve ser configurável para permitir a otimização das configurações de varredura;

3.3.6. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

3.3.7. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

3.3.8. A solução deve se integrar com solução de gerenciamento de acessos privilegiados para autenticação nos dispositivos, no mínimo, os seguintes:

3.3.8.1. CyberArk;

3.3.8.2. BeyondTrust;

3.3.8.3. Thycotic;

3.3.8.4. Centrify;

3.3.9. A solução deve suportar o agendamento de scans personalizados, incluindo a capacidade de executar varreduras em tempos designados, com frequência pré-determinada;

3.3.10. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de scan;

3.3.11. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

3.3.12. A solução deve ser capaz de realizar em tempo real a descoberta de vulnerabilidades nas seguintes tecnologias:

3.3.12.1. Cloud Services;

3.3.12.2. Data Leakage;

3.3.12.3. Database;

3.3.12.4. IoT;

3.3.12.5. Mobile Devices;

3.3.12.6. Operating System;

3.3.12.7. Peer-To-Peer;

3.3.12.8. SCADA;

3.3.12.9. Web Servers;

3.3.12.10. Web Clients;

3.3.13. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

3.3.14. A solução deve em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

3.4. Da análise e priorização de vulnerabilidades

3.4.1. A solução deve ser capaz de exibir ambos severidade e pontuação, com base em CVSS (Common Vulnerability Scoring System) e inteligência de ameaças;

3.4.2. A solução deve utilizar sistema de pontuação e priorização das vulnerabilidades que utilize no mínimo:

3.4.2.1. CVSS Impact Score;

3.4.2.2. Idade da Vulnerabilidade;

3.4.2.3. Maturidade de códigos de exploração da vulnerabilidade encontrada;

3.4.2.4. Frequência de uso da vulnerabilidade em ataques e campanhas atuais;

3.4.2.5. Disponibilidade do código de exploração da vulnerabilidade;

3.4.2.6. Presença de módulos de exploração de vulnerabilidade em frameworks automatizados de exploração de vulnerabilidades como CANVAS, Metasploit e Core Impact;

3.4.2.7. Popularidade da vulnerabilidade em fóruns e comunicações na Darkweb;

3.4.3. O mecanismo de priorização deve ser sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

3.5. Da Inteligência de Vulnerabilidades Centralizada:

3.5.1. A solução deve fornecer acesso integrado e em tempo real a um banco de dados de vulnerabilidades abrangente, alimentado por múltiplas fontes, incluindo:

3.5.1.1. Conhecimento interno do time de pesquisa do fabricante.

3.5.1.2. Avisos de fornecedores/fabricantes de softwares e hardwares.

3.5.1.3. GitHub Advisory Database.

3.5.1.4. National Vulnerability Database (NVD).

3.5.2. Deve ser acessível diretamente pela plataforma de Gestão de Vulnerabilidades, sem a necessidade de ferramentas externas ou integrações complexas.

3.5.3. O banco de dados de vulnerabilidades deve ser atualizado continuamente com as últimas informações de vulnerabilidades, garantindo a detecção de ameaças emergentes.

3.5.4. A solução deve incluir categorias de vulnerabilidades curadas pelo time de pesquisa do fabricante, combinando indicadores de risco conhecidos com insights especializados para destacar as vulnerabilidades mais críticas e relevantes para o ambiente do CONFEA;

3.5.5. Deverá oferecer categorias de vulnerabilidades pré-definidas e atualizadas, permitindo a priorização e ação rápida em relação às vulnerabilidades críticas, conforme as seguintes categorias:

3.5.5.1. Ameaças Emergentes: Identificação e destaque de vulnerabilidades que estão sendo ativamente monitoradas pelo fabricante da solução, devido ao seu potencial de exploração iminente.

3.5.5.2. Vulnerabilidades Conhecidas da CISA (Cybersecurity and Infrastructure Security Agency): Integração com o Catálogo de Vulnerabilidades Conhecidas da CISA, permitindo a identificação e priorização de vulnerabilidades que são conhecidas por serem exploradas ativamente.

3.5.5.3. Exibição das 50 principais vulnerabilidades com base na Classificação de Prioridade do fabricante, levando em consideração a gravidade, a probabilidade de exploração, existência e maturidade do Exploit.

3.5.5.4. Vulnerabilidades Persistentemente Exploradas: vulnerabilidades que são consistentemente exploradas por atores de ameaças ao longo do tempo.

3.5.5.5. Vulnerabilidades exploradas por Ransomware: Identificação de vulnerabilidades que são comumente exploradas em ataques de Ransomware.

3.5.5.6. Vulnerabilidades Recentemente Exploradas: Identificação de vulnerabilidades que receberam cobertura significativa da imprensa e evidências de exploração ativa.

3.5.5.7. Em Destaque nas Notícias: Identificação de vulnerabilidades que foram amplamente relatadas na imprensa, indicando um alto nível de conscientização pública e potencial de exploração.

3.5.6. A solução deve permitir a correlação entre vulnerabilidades conhecidas e a exposição real dos ativos do CONTRATANTE, identificando quais sistemas e aplicações são afetados por vulnerabilidades críticas e baseados em categorias descritas no item 9.5.5 e seus subitens.

3.5.7. Deve fornecer ao administrador a capacidade de filtrar e pesquisar vulnerabilidades com base nas categorias mencionadas no item 9.5.5 e seus subitens, bem como em outros critérios, como gravidade, data de

publicação e ativos afetados.

3.5.8. A solução deve permitir a geração de relatórios e painéis personalizáveis que exibem informações sobre as vulnerabilidades em cada categoria do item 9.5.5, permitindo o monitoramento e a análise da postura de segurança.

3.5.9. Deve fornecer informações sobre os incidentes de segurança recentes associados as vulnerabilidades.

3.6. Da Análise de Risco do Ambiente

3.6.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

3.6.1.1. O cálculo da pontuação dever ser dinâmico e representar o risco de exposição cibernética da organização, baseada nas pontuações de exposição dos ativos, auxiliando na comunicação eficaz do risco cibernético para líderes e partes interessadas.

3.6.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

3.6.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

3.6.4. A solução deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

3.6.5. A solução deve prover visão sobre quais ações de remediação reduzem o maior nível de risco do ambiente;

3.6.6. A solução deve também permitir a visualização de ações de remediação agregadas para visão consolidada de redução de risco;

3.6.7. Deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

3.6.8. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

3.6.9. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

3.6.10. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

3.6.11. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria assim como outras empresas do mercado;

3.6.12. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

3.6.13. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

3.6.14. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

3.6.15. A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;

3.7. Do Gerenciamento da Análise de Ataques exploráveis

3.7.1. Deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK;

3.7.2. Deve identificar qual a criticidade do ataque, em no mínimo: baixo, médio e alto;

3.7.3. Deve permitir a visualização gráfica dos caminhos de ataque, permitindo uma análise detalhada e intuitiva dos vetores de exploração.

3.7.4. Deve prover a evidência relacionada a descoberta do ataque;

3.7.5. Deve mostrar o objeto relacionado ao ataque, de origem e de destino;

3.7.6. Deve apresentar informações detalhadas relacionadas a mitigação para o ataque em análise;

3.7.7. Deve prover quais ferramentas e possíveis *malwares* associados ao ataque;

3.7.8. Deve disponibilizar de forma gráfica via console de gerenciamento as conexões entre os objetos do ataque;

3.7.9. Deve disponibilizar uma biblioteca com ‘Queries’ para a busca de objetos no mínimo os seguintes segmentos:

3.7.9.1. Rede;

3.7.9.2. Endpoint;

3.7.9.3. Active Directory;

3.7.9.4. Permissão;

3.7.9.5. Ransomware;

3.7.9.6. Vetores;

3.7.9.7. Credenciamento;

3.7.10. Deve suportar no mínimo 90 técnicas de ataques;

3.7.11. Deve permitir analisar, ao menos, os seguintes caminhos das superfícies de ataques:

3.7.11.1. Aplicações WEB (DAST);

3.7.11.2. Nuvem;

3.7.11.3. *Active Directory;*

3.7.11.4. Infraestrutura (Desktops, Servidores).

3.7.12. Deve apresentar os resultados em forma ilustrativa (*Dashboard*).

3.7.13. O *Dashboard* deve oferecer uma visão dos seus ativos vulneráveis considerando:

3.7.13.1. Número de ativos críticos vulneráveis;

3.7.13.2. Número de caminhos de ataque que levam a esses ativos críticos;

3.7.13.3. Número de descobertas abertas e sua gravidade;

3.7.13.4. Matriz para visualizar caminhos com diferentes combinações de valores alvo;

3.7.13.5. Lista de tendências de caminhos de ataque.

3.7.14. Deve listar as diferenças entre os intervalos de tempo e mostrar uma seta direcional a fim de indicar se o valor aumentou ou diminuiu.

3.7.15. Deve permitir que o caminho de ataque leve a um ativo crítico.

3.7.16. Deve apresentar o número total alcançado de ativos críticos;

3.7.17. Deve apresentar uma tendência dos caminhos de ataque, listando os caminhos de ataques mais populares.

3.7.18. Deve ser possível identificar o host suspeito;

3.7.19. Deve ser possível identificar o usuário suspeito;

3.7.20. Deve ser possível identificar o IP suspeito;

3.7.21. Deve permitir visualização em modo ilustrativo do caminho de ataque;

3.7.22. Deve ser possível identificar qual a técnica utilizada pelo atacante, tais como:

3.7.22.1. Network Sniffing;

3.7.22.2. LSASS Memory;

3.7.22.3. Remote Desktop Protocol;

3.7.22.4. Exploração de serviços remotos;

3.7.22.5. System Services Discovery;

3.7.22.6. Modificação da Política de Grupo;

3.7.22.7. Mecanismo de Controle de Elevação de Abuso.

3.7.23. Deve permitir a comunicação com o framework MITRE ATT&CK ®.

3.7.24. Deve trazer o número de identificação MITRE ATT&CK para a descoberta;

3.7.25. A descoberta no MITRE ATT&CK deve abordar as seguintes ações:

3.7.25.1. A técnica MITRE ATT&CK associada ao achado.

3.7.25.2. A origem da descoberta.

3.7.25.3. O alvo da descoberta.

3.7.25.4. O status para indicar a ação tomada na descoberta, por exemplo, Em andamento.

3.7.26. Deve ser possível exportar uma descoberta como CSV.

3.7.27. Deve ser possível arquivar uma descoberta.

3.7.28. Deve ser possível ver o histórico do log da descoberta.

3.7.29. Deve permitir alterar o status do caminho de ataque descoberto para, pelo menos:

3.7.29.1. Em Progresso;

3.7.29.2. Em Revisão;

3.7.29.3. Feito;

3.8. Da descoberta de ativos

3.8.1. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

3.8.2. A solução deve disponibilizar modelos de escaneamento de descoberta, ajustável, com os seguintes tipos de scan:

3.8.2.1. Enumeração de Hosts;

3.8.2.2. Identificação de Sistema Operacional (SO);

3.8.2.3. Port Scan (Portas comuns);

3.8.2.4. Port Scan (Todas as portas);

3.8.2.5. Customizado;

3.8.3. A solução deve permitir realizar escaneamento de descoberta customizado podendo ser parametrizado de acordo com a necessidade;

3.8.4. A parametrização do escaneamento de descoberta deve, no mínimo, conter os seguintes requisitos:

3.8.4.1. Descoberta de Host;

3.8.4.2. Ping o host remoto;

3.8.4.3. Usar descoberta rápida;

3.8.4.4. Métodos de ping;

a) 3.8.4.4.1. ARP;

b) 3.8.4.4.2. TCP;

c) 3.8.4.4.3. ICMP;

d) 3.8.4.4.4. UDP;

3.8.4.5. Escaneamento de descoberta de dispositivos de OT/SCADA;

3.8.4.6. Escaneamento de descoberta em redes de impressora;

3.8.4.7. Escaneamento em redes Novell;

3.8.4.8. Tecnologia de Wake-on-LAN;

3.8.5. Port Scanning:

3.8.5.1. Portas;

a) 3.8.5.1.1. Considerar portas não escaneadas como fechadas;

b) 3.8.5.1.2. Range de portas a serem escaneadas;

3.8.5.2. Enumerar Portas locais:

a) 3.8.5.2.1. SSH (netstat);

b) 3.8.5.2.2. WMI (netstat);

c) 3.8.5.2.3. SNMP;

3.8.6. Descoberta de Serviços:

3.8.6.1. Sondar todas as portas para encontrar serviços;

3.8.6.2. Procurar por serviços baseado em SSL/TLS;

3.8.6.3. Enumerar todas as cifras SSL/TLS;

3.8.7. A solução deve realizar descoberta de ativo de forma passiva e adicionado automaticamente na

console de gerenciamento;

3.8.8. A solução deve descobrir passivamente quando um host é adicionado na rede;

3.9. Do Inventário de Ativos e mapeamento de exposição

3.9.1. Deve consolidar todos os ativos da organização em uma única interface, incluindo dispositivos, contas de usuário, softwares, ativos em nuvem e aplicações SaaS, facilitando a análise e gestão centralizada.

3.9.2. A solução deve calcular dinamicamente uma pontuação de exposição para cada ativo, variando de 0 a 1000, indicando o nível de risco associado. Pontuações mais altas representarão maior exposição.

3.9.3. Deve atribuir uma classificação de criticidade a cada ativo, em uma escala de 1 a 10, auxiliando na priorização de medidas de segurança com base na importância do ativo para a organização.

3.9.4. Permitir a criação e aplicação de etiquetas (tags), tanto estáticas quanto dinâmicas, para categorizar e organizar ativos conforme critérios específicos, como localização, função ou nível de risco.

3.9.4.1. As *tags* devem suportar o agrupamento de ativos *on premises*. Recursos em núvem, identidades e aplicações *web*.

3.9.5. A solução deve oferecer a capacidade de adicionar sinais de exposição personalizados para monitorar combinações específicas de riscos que possam impactar a organização, permitindo uma gestão proativa das fraquezas (vulnerabilidades, configurações incorretas e permissões excessivas).

3.9.6. A plataforma deve permitir a integração com fontes de dados externas e ferramentas de terceiros para uma análise mais aprofundada da exposição e remediação de riscos.

3.9.7. Deve garantir que as informações sobre os ativos sejam atualizadas sempre que um ativo é identificado em uma varredura, mantendo a precisão e relevância dos dados no inventário.

3.9.8. Deve possibilitar a detecção de combinações específicas de vulnerabilidades, exposições de identidade e ameaças que, juntas, aumentam significativamente o risco para a organização.

3.9.9. A plataforma deve possuir uma biblioteca de sinais de exposição pré-definidos pelo fabricante da solução, permitindo às equipes de segurança iniciar rapidamente a identificação de cenários de risco críticos.

3.9.10. A solução deve possibilitar criar sinais de exposição personalizados, utilizando consultas específicas ou processamento de linguagem natural (NLP), adaptando a detecção de riscos às necessidades específicas do negócio.

3.9.11. Deve possibilitar o monitoramento contínuo das violações associadas a cada sinal de exposição, com apresentação de tendências e porcentagens de mudança nos últimos 7 dias, auxiliando na identificação de padrões emergentes.

3.9.12. A plataforma de possuir uma listagem detalhada dos ativos afetados por cada sinal de exposição, incluindo informações como nome do ativo, pontuação de exposição e detalhes específicos das fraquezas identificadas.

3.9.13. Deve possuir funcionalidades para arquivar, editar, duplicar ou excluir sinais de exposição personalizados, proporcionando flexibilidade no gerenciamento dos sinais conforme a evolução das necessidades de segurança.

3.9.14. A solução deve utilizar inteligência artificial para fornecer explicações detalhadas sobre cada sinal de exposição e seus ativos impactados, facilitando a compreensão e a tomada de decisões informadas pelas equipes de segurança.

3.9.15. A plataforma deve unificar as informações de inventário de todos os módulos da solução, com integração nativa ou via API, permitindo uma gestão centralizada e integrada das exposições cibernéticas.

3.10. Da avaliação de vulnerabilidade

3.10.1. A solução deve ser capaz de realizar testes sem a necessidade de agentes instalados no dispositivo destino para detecção de vulnerabilidades;

3.10.2. A solução deve detectar e classificar através de severidades, riscos e vulnerabilidades;

3.10.3. A solução deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-los;

3.10.4. A solução deve incluir uma saída detalhada das vulnerabilidades descobertas como versões de DLL esperadas e encontradas;

3.10.5. A solução deve ser compatível com CVE e fornecer pelo menos 10 anos de cobertura CVE;

3.10.6. A solução deve identificar vulnerabilidades especificas para o Active Directory com os seguintes padrões de verificação:

3.10.6.1. Contas administrativas vulneráveis a Kerberoasting attack;

3.10.6.2. Ultilização de criptografia vulnerável com autenticação Kerberos;

3.10.6.3. Contas com pré-autenticação do Kerberos desabilitada;

3.10.6.4. Verificação de usuários com a opção de nunca expirar a senha com a opção habilitada;

3.10.6.5. Verificar validação de fragilidades do tipo “Unconstrained Delegation”;

3.10.6.6. Verificação de “Pre-Windows 2000 Compatible Access”;

3.10.6.7. Verificação de validade de chaves mestras "Kerberos KRBTGT”;

3.10.6.8. Verificação de “SID History Injection”;

3.10.6.9. Verificação de “Printer Bug Exploit”;

3.10.6.10. Verificação de “Primary Group ID”;

3.10.6.11. Verificação de usuários com Passwords em branco;

3.10.7. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

3.10.8. A solução deve ser capaz de iniciar automaticamente serviços de registro remoto em sistemas Windows ao executar uma varredura credenciada;

3.10.9. A solução deve ser capaz de parar automaticamente o serviço de registro remoto em sistemas Windows novamente assim que a varredura estiver completa;

3.10.10. O scanner deve oferecer suporte a *shell seguro* (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;

3.10.11. A solução deve suportar o uso do *netstat* (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

3.10.11.1. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

3.10.12. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows;

3.10.13. A solução deve fornecer auditoria de patch para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;

3.10.14. A solução deve fornecer varredura para aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Trellix, etc;

3.10.15. A solução deve incluir classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade Versão (CVSS2 e CSVSS 3);

3.10.16. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

3.10.17. A solução deve informar se a vulnerabilidade pode e está sendo ativamente explorada por código malicioso (malware);

3.10.18. A solução deve possuir importação de arquivos .YARA;

3.10.19. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

3.11. Da auditoria de Configuração

3.11.1. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

3.11.2. A solução deve fornecer benchmarks de auditoria de segurança e configuração para conformidade regulatória e outros padrões de práticas recomendadas pela área ou fabricantes;

3.11.3. A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes:

3.11.3.1. Center for Internet Security Benchmarks (CIS);

3.11.3.2. Defense Information Systems Agency (DISA) STIGs;

3.11.3.3. Health Insurance Portability and Accountability Act (HIPAA);

3.11.3.4. Payment Card Industry Data Security Standards (PCI DSS);

3.11.4. A solução deve fornecer auditoria de programas antivírus para determinação de presença e status

de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, McAfee VirusScan, Trellix Endpoint Security, Microsoft Endpoint Protection e Kaspersky;

3.11.5. A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;

3.11.6. A solução deve permitir auditoria de conformidade em servidores Windows, Linux, Bancos de Dados SQL Server, a fim de determinar se estão configurados de acordo com os principais Framework de segurança como, por exemplo, CIS e DISA;

3.11.7. A solução deve oferecer validação e suporte a SCAP (Security Content Automation Protocol);

3.12. Da coleta de informações de terceiros

3.12.1. A solução deve oferecer suporte a conectores de terceiros com as seguintes funcionalidades técnicas:

3.12.2. A solução deve suportar uma ampla gama de tipos de conectores, incluindo ferramentas de segurança de endpoint, scanners de nuvem, plataformas de segurança de aplicações (SAST/DAST), ferramentas de gerenciamento de patches e sistemas de gerenciamento de inventário de ativos (CMDBs).

3.12.3. As integrações devem permitir a agregação e correlação de dados de segurança em um único local, fornecendo uma visão unificada da superfície de ataque da organização.

3.12.4. A plataforma deve ser capaz de ingerir dados de ativos (como endpoints, aplicações, recursos em nuvem e código) e vulnerabilidades de plataformas de terceiros.

3.12.5. Deve coletar também metadados associados, como pontuações de risco e tags de negócios, para enriquecer a análise e apoiar a tomada de decisões informadas.

3.12.6. A solução deve agregar dados de ativos e vulnerabilidades de múltiplas ferramentas em um único inventário consolidado.

3.12.7. A solução deve aplicar uma lógica de deduplicação automática para mesclar registros duplicados de diferentes fontes em uma única visão do ativo.

3.12.8. Os critérios de deduplicação padrão devem incluir identificadores de instância de nuvem, endereços MAC, nomes de host, IPs externos, FQDNs e endereços IP.

3.12.9. A solução deve possuir uma lógica de unificação do mesmo ativo mesmo que sejam fornecidas informações de várias fontes, evitando a duplicação.

3.12.10. A plataforma deve adicionar novos dados aos ativos quando os critérios de deduplicação são atendidos.

3.12.11. A solução deve utilizar uma ordem de prioridade fixa de conectores, para que quando fontes múltiplas fornecerem valores conflitantes para a mesma propriedade de um ativo (como IP ou sistema operacional), a informação do conector prioritário seja considerada.

3.12.12. A solução deve permitir a configuração de políticas de retenção para remover automaticamente ativos inativos após um período de tempo definido, com base na data da última varredura. Isso garante que o inventário de ativos permaneça atualizado e relevante, minimizando falsos positivos.

3.12.13. Deve oferecer uma interface para configurar e gerenciar conectores, permitindo a definição de credenciais e a programação da sincronização.

3.12.14. O sistema deve fornecer logs detalhados e status de sincronização para monitorar o progresso da ingestão de dados.

3.12.15. A solução deve suportar a execução de sincronizações para múltiplos conectores simultaneamente, sem a necessidade de esperar que um processo termine antes de iniciar outro.

3.12.16. A solução deve exibir todas as vulnerabilidades relatadas por qualquer um dos conectores que suportam essa função, em um único painel, permitindo a análise e o gerenciamento centralizado de vulnerabilidades de diferentes fontes.

3.12.17. Deve ser possível importar metadados (tags, pontuações de risco) de conectores de terceiros e utilizá-los para pesquisa, filtragem e criação de relatórios dentro da plataforma.

3.12.18. A plataforma deve fornecer uma maneira clara de identificar a origem de cada campo de dados em um ativo (por exemplo, "Origem: Conector AWS"). Isso ajuda os administradores a entenderem de onde as informações estão vindo e a validarem a precisão dos dados.

3.12.19. Deve ter um método seguro para armazenar e gerenciar credenciais de API (tokens, chaves) usadas pelos conectores, garantindo que as integrações sejam autenticadas de forma segura.

3.12.20. Quando um conector é desativado ou removido, a solução deve executar uma rotina de limpeza de

dados em duas etapas. A primeira etapa marca os dados do conector para remoção, e a segunda etapa, durante um processo de limpeza agendado, remove permanentemente todos os dados (ativos, vulnerabilidades e metadados) que foram exclusivamente ingeridos por aquele conector.

3.12.21. A plataforma deve manter dados de ativos que foram mesclados de um conector removido, desde que outros conectores ativos continuem a reportar informações. Isso evita a perda de dados valiosos e garante a continuidade da visão do ativo.

3.12.22. A solução deve ser capaz de processar sincronizações de conectores de forma concorrente, sem a necessidade de enfileirá-las. O primeiro conector que for processado com sucesso torna-se a fonte primária para as decisões de unificação de informações, caso não haja dados de fontes nativas disponíveis.

4. ITEM 2 - LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA APLICAÇÕES WEB

4.1. Cada unidade de software contratada, deverá corresponder a gestão de vulnerabilidade de 1 (um) site WEB da CONTRATANTE.

4.2. O software deverá ser fornecido na modalidade de subscrição e deverá possuir garantia oficial da fabricante da oferta pelo período de 36 (trinta e seis) meses.

4.3. As licenças deverão estar no nome do CONTRATANTE, não serão aceitas licenças utilizadas na prestação de serviços;

4.4. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

4.5. A solução deve ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

4.6. A solução deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

4.7. A solução deve suportar as diretivas PCI ASV 5.5 para definição de escopo de análise da aplicação;

4.8. A solução deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

4.9. A solução deve possuir templates prontos de varreduras entre simples e extensos;

4.10. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

4.10.1. Cookies, Headers, Formulários e Links;

4.10.2. Nomes e valores de parâmetros da aplicação;

4.10.3. Elementos JSON e XML;

4.11. Elementos DOM;

4.12. A solução deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

4.13. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

4.14. A solução deve excluir determinadas URLs da varredura através de expressões regulares;

4.15. A solução deve excluir determinados tipos de arquivos através de suas extensões;

4.16. A solução deve instituir no mínimo os seguintes limites:

4.16.1. Número máximo de URLs para crawl e navegação;

4.16.2. Número máximo de diretórios para varreduras;

4.16.3. Número máximo de elementos DOM;

4.16.4. Tamanho máximo de respostas;

4.16.5. Limite de requisições de redirecionamentos;

4.16.6. Tempo máximo para a varredura;

4.16.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

4.16.8. Número máximo de requisições HTTP por segundo;

4.17. A solução deve detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

4.17.1. Limite em segundos para timeout de requisições de rede;

4.17.2. Número máximo de timeouts antes que a varredura seja abortada;

4.18. A solução deve agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

4.19. A solução deve enviar notificações através de no mínimo E-mail e SMS;

4.20. A solução deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

4.21. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPs;

4.22. A solução deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

4.23. A solução deve ser compatível com avaliação de web services REST e SOAP;

4.24. Deverá suportar no mínimo os seguintes esquemas de autenticação:

4.24.1. Autenticação básica (digest);

4.24.2. NTLM;

4.24.3. Form de *login*;

4.24.4. Autentiçação de Cookies;

4.24.5. Autenticação através de Selenium;

4.24.6. Autenticação através de Bearer;

4.25. A solução deve importar scripts de autenticação selenium previamente configurados pelo usuário;

4.26. A solução deve customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

4.27. A solução deve exibir os resultados das varreduras em tendência temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

4.28. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

4.29. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

4.30. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

4.31. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

4.31.1. Payload injetado;

4.31.2. Evidência em forma de resposta da aplicação;

4.31.3. Detalhes da requisição HTTP;

4.31.4. Detalhes da resposta HTTP;

4.32. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

4.33. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

4.34. A solução deve possuir suporte a varreduras de componentes para no mínimo:

4.35. Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

5. ITEM 3 – LICENCIAMENTO PARA A GESTÃO DE SUPERFÍCIE DE ATAQUE

5.1. Requisitos Gerais

5.2. Cada unidade de software contratada, deverá corresponder a gestão de superfície de ataque de 2 (dois) ativos externo da CONTRATANTE.

5.3. O software deverá ser fornecido na modalidade de subscrição e deverá possuir garantia oficial da fabricante da oferta pelo período de 36 (trinta e seis) meses.

5.4. As licenças deverão estar no nome do CONTRATANTE, não serão aceitas licenças utilizadas na prestação de serviços;

5.4.1. Deve possuir Interface intuitiva com dashboards personalizáveis e relatórios automáticos.

5.4.2. Possuir integração com outras ferramentas de segurança, como SIEMs e plataformas de gerenciamento de vulnerabilidades.

5.4.3. Para varredura aprofundada de uma aplicação web exposta, deve possuir integração para iniciar uma varredura pela solução de DAST da própria plataforma ou possuir integração nativa com a solução de Web Application Scanning fornecido no item 2.

5.4.4. Deve possuir conformidade com normas e padrões de segurança reconhecidos, como ISO 27001, NIST e LGPD.

5.5. Descoberta e Mapeamento de Ativos

5.5.1. Possuir identificação automática e contínua de ativos expostos na internet, incluindo domínios, subdomínios, endereços IP, portas abertas e serviços.

5.5.2. Para detecção de ativos expostos, deve ainda permitir integração com a Cloudflare, AWS, Microsoft Azure e Google Cloud Platform.

5.5.3. Deve ter capacidade de correlacionar ativos a partir de ASN, registros DNS, certificados SSL/TLS e outros dados públicos.

5.5.4. Possuir atualização frequente da superfície de ataque, com ciclos diários ou quinzenais.

5.6. Classificação e Contextualização de Ativos

5.6.1. Deve coletar e possuir organização de metadados de ativos, incluindo versão de software, tecnologias utilizadas e localização geográfica.

5.6.2. Deve possuir filtros avançados para classificação de ativos por risco, tipo e criticidade.

5.6.3. Possuir capacidade de agrupar e categorizar ativos conforme necessidade do órgão contratante.

5.6.4. Deve possuir sensores na Internet para detectar domínios semelhantes com os monitorados pela plataforma. Além disso, deve permitir a adição dos domínios e subdomínios semelhantes encontrados ao inventário da solução.

5.7. Avaliação de Riscos e Detecção de Vulnerabilidades

5.7.1. Deve possuir identificação automática de vulnerabilidades em ativos expostos.

5.7.2. Deve correlacionar bancos de dados de vulnerabilidades públicos e proprietários, como CVE, NVD e outras fontes de ameaças conhecidas.

5.7.3. Deve possuir análise de riscos baseada em criticidade, com recomendações de mitigação priorizadas.

5.7.4. Deve avaliar a postura de segurança e o risco com verificação de vulnerabilidade dos ativos descobertos externos a organização.

5.7.5. Permitir acompanhar as alterações selecionadas, por meio de alertas automáticos, em conformidade, tecnologia e exposição.

5.8. Integração com Plataformas e Automacão:

5.8.1. APIs abertas para integração com sistemas de gerenciamento de vulnerabilidades, SIEMs e plataformas de Threat Intelligence.

5.8.2. Possibilidade de exportação de relatórios em formatos padronizados (CSV, JSON, PDF).

5.8.3. Suporte à automação de respostas a incidentes e workflows de segurança.

5.8.4. Conexão com sistemas de monitoramento de DNS e reputação de IPs para detecção de domínios comprometidos ou maliciosos.

5.8.5. Capacidade de correlacionar dados com feeds de Threat Intelligence, identificando ameaças emergentes associadas aos ativos descobertos.

5.9. Relatórios e Auditoria

5.9.1. Geração automática de relatórios customizáveis para auditorias, conformidade e gestão de riscos.

5.9.2. Deve possuir registros detalhados de todas as ações realizadas na plataforma para fins de auditoria e rastreabilidade.

6. ITEM 4 – LICENCIAMENTO PARA A GESTÃO DE VULNERABILIDADES PARA ACTIVE DIRECTORY

6.1. Cada unidade de *software* contratada, deverá corresponder a gestão de vulnerabilidade de 2 (dois) usuários de Active Directory da CONTRATANTE.

6.2. O software deverá ser fornecido na modalidade de subscrição e deverá possuir garantia oficial da

fabricante da oferta pelo período de 36 (trinta e seis) meses.

6.3. As licenças deverão estar no nome do CONTRATANTE, não serão aceitas licenças utilizadas na prestação de serviços;

6.4. A solução deve identificar fraquezas ocultas em configurações dedicadas ao Active Directory e Entra ID (Microsoft Azure Active Directory);

6.5. A solução deve possuir ações preventivas de *hardening* para o Active Directory;

6.6. A solução deve identificar ataque específicos para a estrutura do Active Directory;

6.7. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta que acarreta riscos de segurança – com uma linguagem simples, contextualizando tal risco para os times envolvidos;

6.8. A solução deve possuir recomendações de correção para cada configuração incorreta no Active Directory;

6.9. A solução deve avaliar relações de confiança perigosas entre florestas e domínios;

6.10. A solução deve capturar as mudanças que ocorrem no AD e demostrar na console de administração;

6.11. A solução deve possuir *dashboard* com os principais ataques e vulnerabilidades por domínio;

6.12. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

6.13. A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;

6.14. A solução deve prover interface web para gerenciamento de todas as funcionalidades;

6.15. A solução deve possuir capacidade nativa de criação de dashboards customizados;

6.16. A solução deve suportar um modelo de controle de acesso baseado em funções (RBAC) flexível;

6.17. A solução não deve realizar alterações no Active Directory, seus objetos e atributos;

6.18. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do Active Directory;

6.19. A solução deve suportar ambientes com múltiplas florestas e domínios;

6.20. A solução deve suportar monitoramento contínuo de ambientes com Active Directory com o nível funcional de floresta e domínio a partir do 2003;

6.21. A solução deve suportar reter os eventos coletados por no mínimo um ano;

6.22. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados com os seguintes padrões:

6.22.1. Não depender de agentes ou sensores para coleta de informações do AD;

6.22.2. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o Active Directory, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;

6.22.3. Interface web que consolida e apresenta de maneira unificada os domínios monitorados e as possíveis relações de confiança estabelecidas entre eles;

6.23. A solução deve analisar continuamente a postura de segurança do AD, minimamente avaliando:

6.23.1. Validação de GPOs desvinculadas, desabilitadas ou órfãs;

6.23.2. Validação de contas desativadas em grupos privilegiados;

6.23.3. Domínio usando uma configuração perigosa de compatibilidade com versões anteriores por meio de alterações no atributo dSHeuristics;

6.23.4. Validação de atributos relacionados a roaming de credenciais vulneráveis (ms-PKI-DPAPIMasterKeys) gerenciados por um usuário sem privilégios;

6.23.5. Validação de domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1;

6.23.6. Validação de contas com senhas que nunca expiram;

6.23.7. Validação de senhas reversíveis em GPOs;

6.23.8. Validação de uso de senhas reversíveis em contas de usuário;

6.23.9. Validação de utilização de protocolo criptográfico fraco (Ex. DES) em contas de usuário;

6.23.10. Validação de uso do LAPS (Solução de senha de administrador local) para gerenciar senhas de

contas locais com privilégios;

6.23.11. Validação se o domínio possui um nível funcional desatualizado;

6.23.12. Validação de contas de usuário utilizando senha antiga;

6.23.13. Validação se o atributo AdminCount está definido em usuários padrão;

6.23.14. Validação do uso recente da conta de administrador padrão;

6.23.15. Validação de usuários com permissão para ingressar computadores no domínio;

6.23.16. Validação de contas dormentes;

6.23.17. Validação de computadores executando um sistema operacional obsoleto;

6.23.18. Validação de restrições de logon para usuários privilegiados em ambiente com múltiplos tiers (1, 2 e 3) de segregação de ativos;

6.23.19. Validação de direitos perigosos configurados no Schema do AD;

6.23.20. Validação de relação de confiança perigosa com outras Florestas e Domínios;

6.23.21. Validação de contas que possuem um atributo perigoso de histórico SID (SID History);

6.23.22. Validação de contas utilizando controle de acesso compatível com versões anteriores ao Windows 2000;

6.23.23. Validação da última alteração de senha do KDC;

6.23.24. Validação da última alteração da senha da conta SSO do Azure AD;

6.23.25. Validação de contas que podem ter senha em branco/vazia;

6.23.26. Validação de utilização do grupo nativo Protected Users;

6.23.27. Validação de privilégios sensíveis (Ex. Debug a program, Replace a process level token, etc.) perigosos atribuídos aos usuários;

6.23.28. Validação de possível senha em clear-text;

6.23.29. Validação de sanidade das GPOs e componentes CSEs (Client-Side Extension);

6.23.30. Validação de uso de algoritmos de criptografia fracos na PKI do Active Directory;

6.23.31. Validação de contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados;

6.23.32. Validação de contas anormais nos grupos administrativos padrão do AD;

6.23.33. Validação de consistência no container adminSDHolder;

6.23.34. Validação de delegação Kerberos perigosa;

6.23.35. Validação em permissões de objetos raiz que permitem ataques do tipo DCSync;

6.23.36. Validação de políticas de senha fracas aplicadas aos usuários;

6.23.37. Validação das permissões relacionadas às contas do Azure AD Connect;

6.23.38. Validação do ID do grupo primário do usuário (Primary Group ID);

6.23.39. Validação de permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;

6.23.40. Controladores de domínio gerenciados por usuários ilegítimos;

6.23.41. Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas;

6.23.42. Validação de uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472);

6.24. A solução deve identificar vulnerabilidades e configurações incorretas do AD à medida que são introduzidas sendo:

6.24.1. Identificar todas as vulnerabilidades e configurações incorretas no AD;

6.24.2. Monitorar relações de confiança perigosas em toda a estrutura AD;

6.24.3. Apresentar ameaças e alterações sem a necessidade de scans estáticos e programados no Active Directory e sua infraestrutura;

6.24.4. Apresentar as ameaças e alterações em tempo real ou em menos de cinco minutos;

6.25. Detecção e resposta a ataques:

6.25.1. Monitorar continuamente os indicadores de possíveis ataque como DCSync, DCShadow, Password

Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros;

6.25.2. Detecção de ataques ao AD em tempo real ou em menos de um minuto;

6.25.3. Análise detalhada do ataque, apresentando ativo de origem, vetor de ataque, controlador de domínio afetado, técnica aplicada;

6.25.4. Apresentação de ataques em uma linha do tempo;

6.25.5. Investigar ameaças, reproduzir ataques e procurar por backdoors;

6.25.6. Permitir busca ágil de eventos específicos na base da solução através de queries customizadas;

6.26. A solução deve ser capaz de enviar alertas por e-mail;

6.27. A solução nativamente deve ser capaz de se integrar com SIEM através de protocolo SYSLOG;

6.28. A solução deve ser capaz de filtrar e enriquecer os eventos que serão enviados para o SIEM;

6.29. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

6.30. A solução deve possuir conjunto de APIs REST, todas as chamadas disponíveis devem estar contidas na documentação;

6.31. A solução deve permitir a criação de listas de exclusões, suportando minimamente Exclusão por domínios do AD monitorados e por itens analisados;

6.32. A solução deve ser licenciada pelo número de usuários habilitados;

6.33. Gerenciamento de Risco de Identidades

6.33.1. Deve classificar identidades do maior para o menor risco, utilizando análises avançadas, otimizando a alocação de recursos e aprimorando a postura geral de segurança.

6.33.2. Deve disponibilizar uma visão aprofundada de cada identidade por meio de múltiplas perspectivas, incluindo contas associadas, fraquezas identificadas, dispositivos conectados, privilégios de acesso e padrões de atividade.

6.33.3. Deve Fornecer insights que permitem às equipes de segurança identificar e remediar vulnerabilidades associadas a identidades de alto risco, implementar políticas de controle de acesso mais eficazes, detectar e responder rapidamente a potenciais ameaças internas.

6.33.4. A solução deve consolidar contas do Active Directory e Entra ID sob uma entidade unificada, utilizando atributos como endereços de e-mail e UPNs para associação precisa.

6.33.5. Deve fornecer *dashboards* para visualização, busca e gestão de informações de identidade, com foco em métricas de segurança como fraquezas e exposição a ataques.

6.33.6. A solução deve avaliar de forma contínua as exposições relacionadas a identidades, como configurações incorretas, permissões excessivas e relacionamentos de confiança arriscados, permitindo a priorização e mitigação de riscos antes que sejam explorados.

6.33.7. Deve possuir sistema de pontuação baseado em inteligência artificial que avalia e classifica cada identidade com base em vulnerabilidades inerentes e riscos herdados, auxiliando na priorização de esforços de remediação.

6.33.8. Possuir capacidade de monitorar continuamente a infraestruturas de identidade híbridas (Active Directory e Entra ID), fornecendo alertas em tempo real sobre novas fraquezas e técnicas avançadas de ataque, permitindo respostas rápidas e eficazes.

6.33.9. Deve possibilitar integração nativa com os módulos de gerenciamento de vulnerabilidade e segurança em Nuvem, permitindo uma visão holística dos riscos relacionados à identidade dentro da superfície geral de ataque da organização.

6.33.10. Deve permitir exportar descobertas e dados em formato .CSV, permitindo personalização das exportações para mostrar colunas específicas conforme necessário.

7. ITEM 5 – SERVIÇO DE INSTALAÇÃO

7.1. Cada unidade adquirida deste item permitirá a instalação integral de 1 (um) dentre os licenciamentos de softwares a serem contratados, Itens 1, 2, 3 ou 4, independentemente do volume de licenças adquiridas.

7.2. A Instalação deverá ser realizada por equipe especializada, com comprovação de experiência em ferramentas de gestão de vulnerabilidades e certificações técnicas aplicáveis.

7.3. A CONTRATADA deverá elaborar um de plano de instalação com escopo técnico detalhado,

identificando fases, responsáveis, requisitos prévios e cronograma.

7.4. Instalação e configuração dos componentes da solução, incluindo:

7.4.1. Console de gerenciamento (*on-premise ou cloud*);

7.4.2. Sensores de varredura (locais e remotos);

7.4.3. Agentes, se aplicável, para estações de trabalho e servidores;

7.4.4. Configuração de credenciais para varreduras autenticadas;

7.5. Deverá efetuar a Integração com serviços de diretório.

7.6. Deverá efetuar a configuração de perfis de varredura, níveis de criticidade, políticas de detecção e janelas de escaneamento compatíveis com a operação do órgão.

7.7. A CONTRATADA deverá efetuar testes de aceitação técnica, incluindo:

7.7.1. Verificação da cobertura de ativos;

7.7.2. Validação da detecção de vulnerabilidades conhecidas;

7.7.3. Teste de performance do scanner e impacto na rede;

7.7.4. Avaliação de falsos positivos.

7.8. CONTRATADA deverá entregar uma documentação técnica com:

7.8.1. Arquitetura lógica da solução implantada;

7.8.2. Configurações realizadas;

7.8.3. Procedimentos operacionais padrão;

7.8.4. Plano de continuidade e recomendações para uso seguro.

8. ITEM 6 – TREINAMENTO POR PLATAFORMA

8.1. Após o término dos procedimentos de instalação, a CONTRATADA deverá executar treinamento na solução implantada.

8.2. Cada turma irá conter no máximo 4 (quatro) participantes;

8.3. Cada sessão de treinamento deverá englobar 1 (um), dentre os *softwares* contratados, sejam eles o Item 1, 2, 3 ou 4.

8.4. O repasse deverá possuir duração mínima de 16 (dezesseis) horas, sendo admitida a sua divisão em 2 (dois) ou 4 (quatro) dias.

8.5. O serviço poderá ser executado pelo mesmo profissional responsável pelos procedimentos de instalação, ou por outro profissional certificado na solução.

8.6. O treinamento deverá ser executado em formato on-line síncrono, de modo remoto.

8.7. O treinamento deverá abordar os seguintes tópicos, minimamente:

8.7.1. Visão geral da arquitetura da solução:

8.7.1.1. Componentes da solução;

8.7.1.2. Topologias comuns;

8.7.1.3. Modalidades de varredura de vulnerabilidades.

8.7.2. Acesso e gerenciamento:

8.7.2.1. Interface de gerenciamento e configuração da solução;

8.7.2.2. Procedimentos de *backup* ou proteção das configurações;

8.7.2.3. Configuração de serviços internos de rede da solução.

8.7.3. Configurações de rede:

8.7.3.1. Interfaces de rede e interconexões;

8.7.3.2. Regras de varredura;

8.7.3.3. Aplicação de funcionalidades correlatas.

8.7.4. Operação:

8.7.4.1. Depuração e troubleshooting;

8.7.4.2. Abertura de chamados;

8.7.4.3. Gerenciamento de licenças.

9. ITEM 7 – SERVIÇO CONTINUADO PARA GESTÃO DE VULNERABILIDADES

9.1. O serviço deverá ser prestado *proativamente* (preventiva) e reativamente (corretiva e evolutiva), na modalidade 24x7x365 (vinte e quatro horas por dia e sete dias por semana) para auxiliar na operação diária da solução contratada pelo CONTRATANTE.

9.2. O serviço deverá atender à um acordo de nível de serviço (SLA) para tempo de atendimento de até 2 (duas) horas após a solicitação, prestado por recurso técnico da CONTRATADA.

9.3. Deverá auxiliar nas questões relativas às atualizações, *patches*, e alertas de impacto, assim como contribuir para o acompanhamento da saúde do ambiente nas atividades diárias.

9.4. Deverá oferecer respostas ou esclarecimentos de dúvidas relacionadas com as soluções do escopo de fornecimento deste Termo de Referência, inclusive em atividades operacionais do dia a dia, reduzindo assim o tempo de inatividade não planejado.

9.5. Deverá executar, durante a vigência do contrato, o serviço de atendimento contínuo, durante 36 (trinta e seis) meses ininterruptos.

9.6. Cada unidade adquirida deste item deverá permitir a execução do rol de atividades previstas neste escopo, por licenciamento de software contratado (Itens 1, 2, 3 e 4 do objeto).

9.6.1. O atendimento contínuo deverá ocorrer de modo remoto e síncrono, entretanto, caso seja solicitado atendimento presencial, caberá a CONTRATADA prover recurso técnico na solução nas dependências do CONTRATANTE.

9.7. O atendimento deverá ser feito por profissional certificado na solução.

9.8. O serviço continuado para gestão de vulnerabilidades terá obrigações para a CONTRATADA com a finalidade de garantir a continuidade e evolução das ferramentas conforme descritivo:

9.8.1. A CONTRATADA deverá realizar auxílio em ajustes e atualizações de novas versões do *software* caso existam novas funcionalidades;

9.8.2. A CONTRATADA deverá auxiliar o contato com a fabricante caso exista alguma interrupção de serviço SaaS;

9.8.3. A CONTRATADA deverá realizar o refinamento de perfis de risco com base em novas vulnerabilidades ou prioridades de negócio;

9.8.4. A CONTRATADA deverá auxiliar na adoção de novos recursos das ferramentas contratadas;

9.8.5. A CONTRATADA deverá verificar continuamente a exposição geral da organização a vulnerabilidades e suas variações, informando o CONTRATANTE de possíveis manobras ou ajustes que devem ser feitos no ambiente;

9.8.6. A CONTRATADA deverá indicar continuamente os ativos com maior impacto e informar sobre mudanças de criticidade dos ativos;

9.8.7. A CONTRATADA deverá analisar os indicadores de exposição por categoria de ativo, rede, localização ou usuário;

9.8.8. A CONTRATADA deverá validar se os ativos mais críticos estão cobertos por varreduras recentes e completas;

9.8.9. A CONTRATADA deverá avaliar a evolução do risco por tendência mensal ou semestral, identificando desvios anormais;

9.8.10. A CONTRATADA deverá informar ao CONTRATANTE se as ações de remediação tomadas pelo CONTRATANTE reduzem o risco de forma mensurável;

9.8.11. A CONTRATADA deverá informar a CONTRATANTE sobre a topologia atualizada dos vetores de ataque gerados pela ferramenta consumida;

9.8.12. A CONTRATADA deverá informar a CONTRATANTE se novos caminhos de ataque surgiram após movimentações de rede ou novas vulnerabilidades;

9.8.13. A CONTRATADA deverá correlacionar os caminhos de ataque com as políticas de acesso e segmentação de rede da CONTRATANTE;

9.8.14. A CONTRATADA deverá garantir que os dados coletados pelas ferramentas estejam sendo sincronizados com as demais soluções integradas.

9.9. A CONTRATADA deverá emitir, semestralmente ou quando solicitada, relatório sobre o panorama de vulnerabilidades identificadas no período, bem como elencar se medidas de contorno foram adotas pela CONTRATANTE.

Documento assinado eletronicamente por **Vinicius de Assis Lima**, **Gerente de Soluções Internas**, em 01/04/2026, às 11:22, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo de Oliveira Coelho Santos**, **Integrante Técnico**, em 01/04/2026, às 11:27, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Carlos Alberto de Azevedo Santos**, **Integrante Administrativo**, em 01/04/2026, às 11:28, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://confea.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1514014** e o código CRC **0C0FDE61**.

Empresa	Fabricante	Item
Empresa 1	Tenable	1
Empresa 1	Tenable	2
Empresa 1	Tenable	3
Empresa 1	Tenable	4
Empresa 1	Tenable	5
Empresa 1	Tenable	6
Empresa 1	Tenable	7
Empresa 2	Tenable/Qualys	1
Empresa 2	Tenable/Qualys	2
Empresa 2	Tenable/Qualys	3
Empresa 2	Tenable/Qualys	4
Empresa 2	Tenable/Qualys	5
Empresa 2	Tenable/Qualys	6
Empresa 2	Tenable/Qualys	7
Empresa 3	Qualys	1
Empresa 3	Qualys	2
Empresa 3	Qualys	3
Empresa 3	Qualys	4
Empresa 3	Qualys	5
Empresa 3	Qualys	6
Empresa 3	Qualys	7
Empresa 4	Qualys	1
Empresa 4	Qualys	2
Empresa 4	Qualys	3
Empresa 4	Qualys	4
Empresa 4	Qualys	5
Empresa 4	Qualys	6
Empresa 4	Qualys	7

Empresa 5	Rapid7	1
Empresa 5	Rapid7	2
Empresa 5	Rapid7	3
Empresa 5	Rapid7	4
Empresa 5	Rapid7	5
Empresa 5	Rapid7	6
Empresa 5	Rapid7	7

Descrição	Unidade	Quantidade
Licenciamento para a Gestão de Vulnerabilidades (36 meses)	UN	11,080
Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	UN	230
Licenciamento para a Gestão de Superfície de Ataque (36 meses)	UN	781
Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	UN	26,380
Serviço de Instalação	UN	16
Treinamento por Solução	UN	16
Serviço Continuado para Gestão de Vulnerabilidades	UN	36
Licenciamento para a Gestão de Vulnerabilidades (36 meses)	UN	11,080
Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	UN	230
Licenciamento para a Gestão de Superfície de Ataque (36 meses)	UN	781
Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	UN	26,380
Serviço de Instalação	UN	16
Treinamento por Solução	UN	16
Serviço Continuado para Gestão de Vulnerabilidades	UN	36
Licenciamento para a Gestão de Vulnerabilidades (36 meses)	UN	11,080
Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	UN	230
Licenciamento para a Gestão de Superfície de Ataque (36 meses)	UN	781
Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	UN	26,380
Serviço de Instalação	UN	16
Treinamento por Solução	UN	16
Serviço Continuado para Gestão de Vulnerabilidades	UN	36
Licenciamento para a Gestão de Vulnerabilidades (36 meses)	UN	11,080
Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	UN	230
Licenciamento para a Gestão de Superfície de Ataque (36 meses)	UN	781
Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	UN	26,380
Serviço de Instalação	UN	16
Treinamento por Solução	UN	16
Serviço Continuado para Gestão de Vulnerabilidades	UN	36

Licenciamento para a Gestão de Vulnerabilidades (36 meses)	UN	11,080
Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	UN	230
Licenciamento para a Gestão de Superfície de Ataque (36 meses)	UN	781
Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	UN	26,380
Serviço de Instalação	UN	16
Treinamento por Solução	UN	16
Serviço Continuado para Gestão de Vulnerabilidades	UN	36

Valor Unitário (R$)	Valor Total (R$)
R$ 1,426.70	R$ 15,807,827.84
R$ 22,832.87	R$ 5,251,560.96
R$ 1,060.67	R$ 785,958.34
R$ 1,001.20	R$ 26,411,752.75
R$ 62,095.24	R$ 993,523.89
R$ 30,398.97	R$ 486,383.52
R$ 34,008.04	R$ 1,224,289.59
R$ 1,343.53	R$ 14,886,320.61
R$ 21,704.04	R$ 4,991,928.20
R$ 989.45	R$ 733,180.69
R$ 960.16	R$ 25,328,965.07
R$ 59,772.55	R$ 956,360.85
R$ 28,433.86	R$ 454,941.73
R$ 32,194.38	R$ 1,158,997.79
R$ 1,267.69	R$ 14,046,008.13
R$ 20,531.23	R$ 4,722,183.68
R$ 933.73	R$ 691,891.52
R$ 894.28	R$ 23,590,977.29
R$ 56,410.77	R$ 902,572.34
R$ 27,364.06	R$ 437,824.97
	R$ 1,080,816.65
R$ 1,298.47	R$ 14,387,059.88
R$ 21,015.97	R$ 4,833,672.24
R$ 965.70	R$ 715,581.69
R$ 931.47	R$ 24,572,232.60
R$ 57,456.48	R$ 919,303.65
R$ 28,097.35	R$ 449,557.58
R$ 31,448.47	R$ 1,132,145.03

R$ 1,379.35	R$ 15,283,210.14
R$ 22,295.59	R$ 5,127,985.29
R$ 1,022.07	R$ 757,352.92
R$ 977.08	R$ 25,775,309.16
R$ 61,605.64	R$ 985,690.32
R$ 29,355.71	R$ 469,691.38
R$ 33,159.96	R$ 1,193,758.43

Pesquisa de Preços (ETP) – Comparativo item a item (36 meses)

Item	Descrição	Qtde	Empresa 1
1	Licenciamento para a Gestão de Vulnerabilidades (36 meses)	11,080	R$ 15,807,827.84
2	Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	230	R$ 5,251,560.96
3	Licenciamento para a Gestão de Superfície de Ataque (36 meses)	781	R$ 785,958.34
4	Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	26,380	R$ 26,411,752.75
5	Serviço de Instalação	16	R$ 993,523.89
6	Treinamento por Solução	16	R$ 486,383.52
7	Serviço Continuado para Gestão de Vulnerabilidades	144	R$ 1,224,289.59
		TOTAL	**R$ 50,961,296.89**

Empresa 2	Empresa 3	Empresa 4	Empresa 5	Média
R$ 14,886,320.61	R$ 14,046,008.13	R$ 14,387,059.88	R$ 15,283,210.14	R$ 14,882,085.32
R$ 4,991,928.20	R$ 4,722,183.68	R$ 4,833,672.24	R$ 5,127,985.29	R$ 4,985,466.07
R$ 733,180.69	R$ 691,891.52	R$ 715,581.69	R$ 757,352.92	R$ 736,793.03
R$ 25,328,965.07	R$ 23,590,977.29	R$ 24,572,232.60	R$ 25,775,309.16	R$ 25,135,847.37
R$ 956,360.85	R$ 902,572.34	R$ 919,303.65	R$ 985,690.32	R$ 951,490.21
R$ 454,941.73	R$ 437,824.97	R$ 449,557.58	R$ 469,691.38	R$ 459,679.84
R$ 1,158,997.79	R$ 1,080,816.65	R$ 1,132,145.03	R$ 1,193,758.43	R$ 1,158,001.50
R$ 48,510,694.94	**R$ 45,472,274.58**	**R$ 47,009,552.67**	**R$ 49,592,997.64**	**R$ 48,309,363.34**

Mínimo	Máximo	Média (sem min/máx)
R$ 14,046,008.13	R$ 15,807,827.84	R$ 14,852,196.88
R$ 4,722,183.68	R$ 5,251,560.96	R$ 4,984,528.58
R$ 691,891.52	R$ 785,958.34	R$ 735,371.77
R$ 23,590,977.29	R$ 26,411,752.75	R$ 25,225,502.28
R$ 902,572.34	R$ 993,523.89	R$ 953,784.94
R$ 437,824.97	R$ 486,383.52	R$ 458,063.56
R$ 1,080,816.65	R$ 1,224,289.59	R$ 1,161,633.75
R$ 45,472,274.58	**R$ 50,961,296.89**	**R$ 48,371,081.75**

Resumo – Pesquisa de Preços (ETP)

Propostas (Valor Total – 36 meses)

Empresa	Fabricante	Valor Total (R$)	Menor?	Maior?
Empresa 1	Tenable	R$ 50,961,296.89		SIM
Empresa 2	Tenable/Qualys	R$ 48,510,694.94		
Empresa 3	Qualys	R$ 45,472,274.58	SIM	
Empresa 4	Qualys	R$ 47,009,552.67		
Empresa 5	Rapid7	R$ 49,592,997.64		

Estatísticas (totais)

Média	R$ 48,309,363.34
Mediana	R$ 48,510,694.94
Mínimo	R$ 45,472,274.58
Máximo	R$ 50,961,296.89
Desvio padrão	#NAME?
Média (sem min/máx)	R$ 48,371,081.75

Obs.: 'Média (sem min/máx)' remove o menor e o maior valor para reduzir efeito de outliers.

Fonte
1443270
1443271
1443273
1443274
1443275

Item c	Especificação	Quantidade
1	Licenciamento para a Gestão de Vulnerabilidades (36 meses)	11080
2	Licenciamento para a Gestão de Vulnerabilidades para Aplicações Web (36 meses)	230
3	Licenciamento para a Gestão de Superfície de Ataque (36 meses)	781
4	Licenciamento para a Gestão de Vulnerabilidades para Active Directory (36 meses)	26380
5	Serviço de Instalação	16
6	Treinamento por Solução	16
7	Serviço Continuado para Gestão de Vulnerabilidades	144

Valor Unitário (36 meses)	Valor Final (36 meses)
R$ 1,343.15	R$ 14,882,085.32
R$ 21,675.94	R$ 4,985,466.07
R$ 943.40	R$ 736,793.03
R$ 952.84	R$ 25,135,847.37
R$ 59,468.14	R$ 951,490.21
R$ 28,729.99	R$ 459,679.84
R$ 8,041.68	R$ 1,158,001.50
	R$ 48,309,363.34

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA – CONFEA

MINUTA - ATA DE REGISTRO DE PREÇOS

Processo: 00.003608/2024-71
Tipo de Processo: Aquisição/Contratação: Bens ou Serviços
Assunto: Fornecimento de Software/Serviço de Gestão de Vulnerabilidades
Interessado: Setor de Infraestrutura e Arquitetura

EDITAL DO PREGÃO ELETRÔNICO Nº 900xx/2026
ANEXO III

ATA DE REGISTRO DE PREÇOS Nº XXX

O **Conselho Federal de Engenharia e Agronomia - CONFEA**, com sede no SEPN 508, Bloco A, Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho, Asa Norte, Brasília - DF, CEP: 70740-541, inscrito(a) no CNPJ nº 33.665.647/0001-91, neste ato representado(a) pelo(a) ....., considerando o julgamento da licitação na modalidade de Pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº ...../202..., publicada no ..... de ...../...../202....., processo administrativo n.º 00.003608/2024-71, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para a eventual contratação de solução de tecnologia da informação e comunicação para gerenciamento de exposição, compreendendo licenciamento de *software*, serviços especializados, suporte técnico, treinamento e serviços continuados, especificado(s) do Termo de Referência, anexo I do edital de licitação n.º xxxx/xxxx, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. O preço registrado , as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item do TR	Fornecedor *[razão social, CNPJ/MF, endereço, contatos, representante]*				
X	**Especificação**	**Unidade**	**Quantidade**	**Valor Unitário**	**Valor Total**

2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1. O órgão gerenciador será o Conselho Federal de Engenharia e Agronomia - CONFEA.

3.2. Além do gerenciador, são órgãos e entidades públicas participantes do registro de preços, conforme itens e quantitativos previstos no Termo de Referência :

a) **Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome – MDS**

b) **Secretaria de Estado da Educação de Rondônia – SEDUC/RO**

c) **Instituto de Desenvolvimento Florestal e da Biodiversidade do Estado do Pará – IDEFLOR-Bio/PA**

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

4.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

4.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e

4.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.

4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

5. DOS LIMITES PARA AS ADESÕES

5.1. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

5.2. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.

5.3. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias,

não ficando sujeita ao limite de que trata o item 4.1., desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021.

6. VEDAÇÃO A ACRÉSCIMO DE QUANTITATIVOS

6.1. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

7. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

7.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

7.1.1. Em caso de prorrogação da ata, poderá ser renovado o quantitativo originalmente registrado.

7.1.2. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

7.1.3. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

7.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

7.2.1. O instrumento contratual de que trata o item 7.2. deverá ser assinado no prazo de validade da ata de registro de preços.

7.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

7.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

7.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

7.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

7.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

7.4.2.2. Mantiverem sua proposta original.

7.4.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

7.5. O registro a que se refere o item 7.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

7.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

7.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o

item 7.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

7.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

7.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 11.

7.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

7.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

7.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

7.10. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

7.11. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 7.7, observando o item 5.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

7.12. Na hipótese de nenhum dos licitantes que trata o item 7.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

7.12.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

7.12.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

7.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

8. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

8.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

8.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021 ;

8.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

8.1.3. Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de

reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

8.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

8.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

9. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

9.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

9.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

9.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

9.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

9.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

9.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

9.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

9.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 11.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

9.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 7.7.

9.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 9.4, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

9.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 9.2 e no item 9.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

9.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que

tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

10. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

10.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

10.2. O remanejamento somente poderá ser feito:

10.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

10.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

10.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

10.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023 .

10.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

10.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

10.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

11. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

11.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

11.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

11.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

11.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

11.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

11.1.4.1. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

11.2. O cancelamento de registros nas hipóteses previstas no item 11.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

11.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

11.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

11.4.1. Por razão de interesse público;

11.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

11.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

12. DAS PENALIDADES

12.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital.

12.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

12.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, IX, do Decreto nº 11.462, de 2023).

12.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 11.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

13. CONDIÇÕES GERAIS

13.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, anexo ao edital.

13.2. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

13.3. Para firmeza e validade do pactuado, a presente Ata foi lavrada em .... (....) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos demais órgãos participantes.

13.4. Local e data

13.5. Assinaturas

13.6. Representante legal do órgão gerenciador e representante(s) legal(is) do(s) fornecedor(s) registrado(s)

Documento assinado eletronicamente por **Irandiaya do Vale Nobre Bandeira Santos**, **Gerente de Contratações**, em 05/03/2026, às 12:31, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

ANEXOS À MINUTA - ATA DE REGISTRO DE PREÇOS

ANEXO I

Cadastro Reserva

Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais ao adjudicatário:

Item do TR	Fornecedor *[razão social, CNPJ/MF, endereço, contatos, representante]*							
X	Especificação	Marca *(se exigida no edital)*	Modelo *(se exigido no edital)*	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Unitário	Prazo garantia ou validade

Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Item do TR	Fornecedor *[razão social, CNPJ/MF, endereço, contatos, representante]*							
X	Especificação	Marca *(se exigida no edital)*	Modelo *(se exigido no edital)*	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Unitário	Prazo garantia ou validade

SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

SEPN 508, Bloco A Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho - Bairro Asa Norte, Brasília/DF, CEP 70740-541

Contato: - http://www.confea.org.br

MINUTA - CONTRATO

Processo: 00.003608/2024-71
Tipo de Processo: Aquisição/Contratação: Bens ou Serviços
Assunto: Fornecimento de Software/Serviço de Gestão de Vulnerabilidades
Interessado: Setor de Infraestrutura e Arquitetura

EDITAL DO PREGÃO ELETRÔNICO Nº 9000X/2026
ANEXO III

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI O CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA E .....

O **CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - Confea**, com sede no(a) SEPN 508, Bloco A Ed. Confea - Engenheiro Francisco Saturnino de Brito Filho - Asa Norte, CEP: 70740-541, Brasília - DF, inscrito(a) no CNPJ sob o nº 33.665.647/0001-91, neste ato representado pelo ....., doravante denominado CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., em ..... doravante designado CONTRATADO, neste ato representado(a) por ..... (nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº ..... e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. .../..., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação para gerenciamento de exposição, compreendendo licenciamento de *software*, serviços especializados, suporte técnico, treinamento e serviços continuados, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato, prorrogável sucessivamente por até 10 anos, na forma dos arts. 106 e 107 da Lei n° 14.133, de 2021.

2.2. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação e nos demais aspectos que forem julgados relevantes, atentando, ainda, para o cumprimento dos seguintes requisitos:

2.2.1. Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

2.2.2. Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

2.2.3. Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

2.2.4. Haja manifestação expressa do CONTRATADO informando o interesse na prorrogação;

2.2.5. Seja comprovado que o CONTRATADO mantém as condições iniciais de habilitação; e

2.2.6. Não haja registro no Cadastro Informativo de créditos não quitados do setor público federal (Cadin).

2.3. O CONTRATADO não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando o CONTRATADO tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. As regras sobre a subcontratação do objeto são aquelas estabelecidas no Termo de Referência, anexo a este Contrato.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor total da contratação é de R$ xxxxxx (xxxxxxxxx).

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

6. CLÁUSULA SEXTA - PAGAMENTO

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE

7.1. As regras acerca do reajuste do valor contratual são aquelas definidas no Termo de Referência, anexo a este Contrato.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1. São obrigações do CONTRATANTE:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo CONTRATADO, de acordo com o contrato e seus anexos;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o CONTRATADO, por escrito, sobre vícios, defeitos, incorreções, imperfeições, falhas ou irregularidades verificadas na execução do objeto contratual, fixando prazo para que seja substituído, reparado ou corrigido, total ou parcialmente, às suas expensas, certificando-se de que as soluções por ele propostas sejam as mais adequadas;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo CONTRATADO;

8.1.5. Comunicar a empresa para emissão de Nota Fiscal relativa à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao CONTRATADO do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao CONTRATADO as sanções previstas na lei e neste Contrato;

8.1.8. Não praticar atos de ingerência na administração do CONTRATADO, tais como:

8.1.8.1. indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

8.1.8.2. fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo CONTRATADO;

8.1.8.3. estabelecer vínculo de subordinação com funcionário do CONTRATADO;

8.1.8.4. definir forma de pagamento mediante exclusivo reembolso dos salários pagos;

8.1.8.5. demandar a funcionário do CONTRATADO a execução de tarefas fora do escopo do objeto da contratação; e

8.1.8.6. prever exigências que constituam intervenção indevida da Administração na gestão interna do CONTRATADO.

8.1.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo CONTRATADO;

8.1.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste;

8.1.10.1. A Administração terá o prazo de 30 (trinta) dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo CONTRATADO no prazo máximo de 30 (trinta) dias;

8.1.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais;

8.1.13. Comunicar o CONTRATADO na hipótese de posterior alteração do projeto pelo CONTRATANTE, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo CONTRATADO com terceiros, ainda que

vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do CONTRATADO, de seus empregados, prepostos ou subordinados.

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO

9.1. O CONTRATADO deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

9.3. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo CONTRATANTE, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

9.5. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o CONTRATADO deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

9.5.1. prova de regularidade relativa à Seguridade Social;

9.5.2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

9.5.3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do CONTRATADO;

9.5.4. Certidão de Regularidade do FGTS – CRF; e

9.5.5. Certidão Negativa de Débitos Trabalhistas – CNDT.

9.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao CONTRATANTE e não poderá onerar o objeto do contrato;

9.7. Comunicar ao Fiscal do contrato tempestivamente, observada a urgência da situação, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual, não ultrapassando o prazo de 24 (vinte e quatro) horas;

9.8. Paralisar, por determinação do CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

9.9. Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação ou para qualificação na contratação direta;

9.10. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação;

9.11. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas;

9.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

9.14. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do CONTRATANTE;

9.15. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados;

9.16. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos;

9.17. Fornecer todos os materiais, equipamentos, ferramentas e utensílios demandados, em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação de regência;

9.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina;

9.19. Submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

9.20. Cumprir as normas de proteção ao trabalho, inclusive aquelas relativas à segurança e à saúde no trabalho;

9.21. Não submeter os trabalhadores a condições degradantes de trabalho, jornadas exaustivas, servidão por dívida ou trabalhos forçados;

9.22. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos de idade, exceto na condição de aprendiz para os maiores de quatorze anos de idade, observada a legislação pertinente;

9.23. Não submeter o menor de dezoito anos de idade à realização de trabalho noturno e em condições perigosas e insalubres e à realização de atividades constantes na Lista de Piores Formas de Trabalho Infantil, aprovada pelo Decreto nº 6.481, de 12 de junho de 2008;

9.24. Receber e dar o tratamento adequado a denúncias de discriminação, violência e assédio no ambiente de trabalho;

9.25. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato;

9.25.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.26. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do CONTRATANTE ou de agente público que tenha desempenhado função na licitação ou que atue na

fiscalização ou gestão do contrato, nos termos do art. 48, parágrafo único, da Lei nº 14.133, de 2021;

9.27. Prestar todo esclarecimento ou informação solicitada pelo CONTRATANTE ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.28. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

9.29. Assegurar aos seus trabalhadores ambiente de trabalho e instalações em condições adequadas ao cumprimento das normas de saúde, segurança e bem-estar no trabalho;

9.30. Fornecer equipamentos de proteção individual (EPI) e equipamentos de proteção coletiva (EPC),quando for o caso;

9.31. Garantir o acesso do CONTRATANTE, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do contrato;

9.32. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;

9.33. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

9.34. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo o CONTRATADO relatar ao CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

10. CLÁUSULA DÉCIMA- OBRIGAÇÕES PERTINENTES À LGPD

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

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

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

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

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

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

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

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

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

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

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO

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

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

12.1. As regras acerca de infrações e sanções administrativas referentes à execução do contrato são aquelas definidas no Termo de Referência, anexo a este Contrato.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Nesta hipótese, aplicam-se também os arts. 138 e 139 da mesma Lei.

13.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.5.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido de:

13.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2. Relação dos pagamentos já efetuados e ainda devidos;

13.6.3. Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório.

13.8. O CONTRATANTE poderá ainda:

13.8.1. nos casos de obrigação de pagamento de multa pelo CONTRATADO, reter a garantia prestada a ser executada, conforme legislação que rege a matéria; e

13.8.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do CONTRATADO decorrentes do contrato.

13.9. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou na contratação direta ou que atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA - ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

14.2. O CONTRATADO é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. 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.

14.4. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do CONTRATANTE, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês.

14.5. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

15. CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do xxxxx deste exercício, na dotação abaixo discriminada:

I - Gestão/Unidade:

II - Fonte de Recursos:

III - Programa de Trabalho:

IV - Elemento de Despesa:

V - Plano Interno:

VI - Nota de Empenho:

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

16. CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

18. CLÁUSULA DÉCIMA OITAVA– FORO

18.1. Fica eleito o Foro da Justiça Federal em ....., Seção Judiciária de ..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

[Local], [dia] de [mês] de [ano].

_____
Representante legal do CONTRATANTE

_____
Representante legal do CONTRATADO
TESTEMUNHAS:
1-
2-

Documento assinado eletronicamente por **Irandiaya do Vale Nobre Bandeira Santos**, **Gerente de Contratações**, em 05/03/2026, às 12:31, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.