Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO

VALOR ESTIMADO PÚBLICO

MENOR PREÇO

FORNECIMENTO DE SERVIÇOS ESPECIALIZADOS DE TESTE DE INVASÃO (PENTEST) E DA CAMPANHA DE CONSCIENTIZAÇÃO PARA CODEVASF.

NOVEMBRO/2025

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ÍNDICE

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Fornecimento de serviços especializados de teste de invasão (pentest) e campanha de conscientização para CODEVASF. Abrangendo avaliação de vulnerabilidades, execução de testes em aplicações, estações de trabalho, infraestrutura de rede, servidores, roteadores, switches, wi-fi e outros dispositivos.

1.2. As especificações detalhadas do objeto desta licitação e suas garantias estão descritos no anexo III do Termo de Referência.

Tabela 1

ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE DE MEDIDA	QUANTIDADE
1	Serviços de Consultoria em Segurança de Tecnologia da Informação e Comunicação (TIC) - Análise de vulnerabilidades e testes de intrusão (pentest) e Campanha de conscientização para CODEVASF.	27340	Unidade de Serviço Técnico	100

1.3. O item é único e aberto para participação de todas as empresas.

1.4. Estimativas de ativos a serem tratados no pentest constam na tabela 2:

Tabela 2

Ativos	Quantidade
Estações de Trabalho (desktops e notebooks)	2200
Servidores on-premises (virtualizados e físicos)	200
Aplicações Web	130
Roteadores	19
Switches	92
Rede Wi-Fi	18
Outros Dispositivos	20
Total	2679

2. TERMINOLOGIAS E DEFINIÇÕES

Neste Termo de Referência (TR) ou em quaisquer outros documentos relacionados com os serviços acima solicitados, os termos ou expressões têm o seguinte significado e/ou interpretação:

ÁREA DE ADMINISTRAÇÃO E TECNOLOGIA – Unidade da administração superior da CODEVASF, à qual estão afetas as demais unidades técnicas que têm por competência a fiscalização e a coordenação dos fornecimentos/serviços de tecnologia da informação, objetos deste Termo de Referência.

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

AA/GTI ou GTI – Gerência de Tecnologia da Informação da Área de Administração e Tecnologia da CODEVASF.

AA/GTI/UIT ou UIT – Unidade de Infraestrutura de TI, subordinada à Gerência de Tecnologia da Informação.

AA/GTI/USC ou USC – Unidade de Segurança Cibernética, subordinada à Gerência de Tecnologia da Informação.

BLACK BOX – Teste realizado sem nenhum conhecimento prévio do ambiente, sistemas ou código-fonte. O teste parte de um local externo, simulando ataques reais a partir de informações públicas ou descobertas durante o teste.

CATMAT – É um módulo do SIASG denominado Sistema de Catalogação de materiais, onde é realizada a inclusão de itens, bem como a sua consulta. Todos os procedimentos para a sua utilização constam dos Manuais disponíveis no Portal de Compras do Governo Federal: www.gov.br/compras**.**

CATSER – É um módulo do SIASG denominado Sistema de Catalogação de serviços, onde é realizada a inclusão de itens, bem como a sua consulta. Todos os procedimentos para a sua utilização constam dos Manuais disponíveis no Portal de Compras do Governo Federal: www.gov.br/compras.

CODEVASF – Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba – Empresa pública vinculada ao Ministério da Integração Nacional, com sede no Setor de Grandes Áreas Norte, Quadra 601 – Lote 1 – Brasília-DF.

CONTRATO – Documento, subscrito pela CODEVASF e a CONTRATADA vencedora do certame, que define as obrigações e direitos de ambas com relação à execução dos fornecimentos.

CONTRATADA – Empresa licitante selecionada e CONTRATADA pela CODEVASF para a execução dos serviços.

DOCUMENTOS DE CONTRATO – Conjunto de todos os documentos que integram o contrato e regulam a execução dos serviços, compreendendo o Edital, Termo de Referência, especificações técnicas, desenhos e proposta financeira da executante, cronogramas e demais documentos complementares que se façam necessários à execução dos serviços.

DOCUMENTOS COMPLEMENTARES ou SUPLEMENTARES – Documentos que, por força de condições técnicas imprevisíveis, se fizerem necessários para a complementação ou suplementação dos documentos emitidos no Termo de Referência.

ESPECIFICAÇÃO TÉCNICA – Tipo de norma destinada a fixar as características dos serviços, condições ou requisitos exigíveis para matérias-primas, produtos semifabricados, elementos de construção, materiais ou produtos industriais semifabricados. Conterá a definição do serviço, descrição do método construtivo, controle tecnológico e geométrico e norma de medição e pagamento.

FISCALIZAÇÃO – Equipe da CODEVASF atuando sob a autoridade de um Coordenador, indicada para exercer em sua representação a fiscalização do contrato.

GRAY BOX – Teste realizado com conhecimento parcial do ambiente ou do sistema. O avaliador recebe informações limitadas, como credenciais de usuário comum ou diagramas de alto nível, possibilitando simular um atacante que já possui algum acesso inicial ou conhecimento interno restrito.

LICITANTE – Empresa habilitada para apresentar proposta.

PDTI: Plano Diretor de Tecnologia da Informação é resultado do detalhamento das ações decorrentes do Planejamento Estratégico da Tecnologia da Informação - PETI, de forma a consolidar todas as iniciativas, metas e os indicadores da área de

Tecnologia da Informação, dando visibilidade às ações, prazos e custos necessários para alcance dos objetivos estratégicos definidos e, ainda, assegurando que estas ações agreguem valor ao negócio da CODEVASF.

PETI: Plano Estratégico de Tecnologia da Informação é o instrumento que tem por objetivo assegurar que as metas e objetivos da TI estejam fortemente alinhados com o Planejamento Estratégico da CODEVASF.

PENTEST – Teste de intrusão controlado e autorizado, realizado para identificar e explorar vulnerabilidades em sistemas, redes ou aplicações. Seu objetivo é avaliar a postura de segurança da organização, simulando ataques reais e apresentando recomendações de mitigação.

PROPOSTA FINANCEIRA – Documento gerado pelo licitante que estabelece os valores unitário e global dos serviços e fornecimentos, apresentando todo o detalhamento dos custos e preços unitários propostos.

SIASG - é um conjunto informatizado de ferramentas para operacionalizar internamente o funcionamento sistêmico das atividades de gestão de materiais, edificações públicas, veículos oficiais, comunicações administrativas, licitações e contratos. É utilizado por várias entidades da Administração Pública Federal (Ministérios, Secretarias, etc.). Pode ser acessado pelo site do Compras Governamentais: www.comprasgovernamentais.gov.br.

SUPERINTENDÊNCIA REGIONAL ou SR – Unidade executiva descentralizada subordinada diretamente à presidência da CODEVASF, em cuja jurisdição territorial localiza-se parte dos fornecimentos objeto deste Termo de Referência.

TERMO DE REFERÊNCIA – conjunto de elementos necessários e suficientes, com nível de precisão adequado, para caracterizar a licitação e subsidiar a elaboração do edital e fornecer informações ao licitante.

UNIDADE DE SERVIÇO TÉCNICO (UST) – Métrica utilizada em contratos de tecnologia para mensurar e precificar atividades técnicas. Representa uma unidade padrão de esforço ou serviço prestado, permitindo quantificar entregas e facilitar a comparação, o planejamento e a cobrança de serviços especializados.

WHITE BOX – Teste realizado com conhecimento completo do ambiente, sistemas e código-fonte. O avaliador tem acesso a diagramas, configurações e documentação técnica, permitindo uma análise minuciosa e abrangente de vulnerabilidades tanto em nível de infraestrutura quanto de aplicação.

3. FORMA DE REALIZAÇÃO, VALOR ESTIMADO E CRITÉRIO DE JULGAMENTO

3.1. A presente licitação é composta por item único, do tipo menor preço, na modalidade de pregão eletrônico com fundamento legal nos preceitos do direito público, em especial, as disposições do estatuto jurídico da empresa pública, Lei nº 13.303, de 30/06/2016, Regulamento Interno de Licitações e Contratos, Lei nº 10.520, de 17/07/2002 que regulamenta a licitação na modalidade de Pregão Eletrônico, e demais exigências deste Termo de Referência e seus anexos que integram o presente.

3.2. **Valor estimado**: Público

3.4. **Critério de Julgamento**: Menor Preço Global

3.5. **Forma de Fornecimento**: Parcelado, conforme descrito no item 14 e seus subitens deste Termo de Referência.

4. LOCAL DE ENTREGA

4.1. Os serviços objeto deste Termo de Referência deverão ser executados/entregues na sede da CODEVASF, localizado em Brasília, no Distrito Federal, conforme ANEXO III.

4.2. A CODEVASF está localizada no endereço: SGAN 601, Módulo I, Edifício Manoel Novaes, Asa Norte CEP: 70830-019 – Brasília/DF.

5. DESCRIÇÃO DOS SERVIÇOS

5.1. O objeto do presente pregão compreende a contratação de serviços de consultoria especializada em testes de intrusão (Pentest) em aplicações e serviços, e campanha de conscientização, conforme a Tabela 1, no item 1.2, deste Termo de Referência.

5.2. A descrição dos serviços consta da planilha de quantidades e preços orçados, e as Especificações Técnicas estão presentes no Anexo III deste Termo de Referência, que deverão ser observadas criteriosamente pelos licitantes.

5.2.1. Havendo divergência entre a descrição dos serviços no sistema ComprasNet e a descrição contida na planilha, prevalecerá a contida na planilha orçamentária.

6. CONDIÇÕES DE PARTICIPAÇÃO

6.1. Poderão participar da presente licitação empresas do ramo, pertinente e compatível com o objeto desta licitação, nacionais ou estrangeiras, que atendam às exigências do Termo de Referência - TR e seus anexos.

6.1.1. As Empresas estrangeiras poderão participar nas mesmas condições das empresas nacionais.

6.2. CONSÓRCIO

6.2.1. Não será permitida a participação de consórcio.

6.3. SUBCONTRATAÇÃO

6.3.1. Não será permitida a subcontratação total ou parcial do objeto desta licitação.

6.4 PARTICIPAÇÃO DE MICROEMPRESA E DE EMPRESA DE PEQUENO PORTE

6.4.1 As Microempresas e as Empresas de Pequeno Porte poderão participar desta licitação em condições diferenciadas, na forma prescrita na Lei Complementar nº 123, de 14 de dezembro de 2006 e Decreto 8.538 de 6/10/2015.

7. VISITA AO LOCAL DA ENTREGA

7.1. O atestado de visita aos locais da execução não será obrigatório, porém, é de inteira responsabilidade do licitante tomar pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos a serem executados, avaliando os problemas futuros, bem como a verificação das dificuldades e dimensionamento dos dados indispensáveis à apresentação da proposta e execução do contrato. A não verificação dessas dificuldades não poderá ser avocada no desenrolar dos trabalhos como fonte de alteração dos termos contratuais que venham a ser estabelecidos. Entende-se que os custos propostos cobrirão quaisquer dificuldades decorrentes da localização do projeto.

7.1.1. Os custos de visita ao local onde serão executados os serviços correrão por exclusiva conta do licitante.

7.1.2. A visita ao local onde serão executados os serviços deverá ser marcada com antecedência mínima de 48 (quarenta e oito) horas e deverá ser realizada em dias úteis de expediente na CODEVASF no horário compreendido entre 09:00 horas às 12:00 horas e das 14:00 horas às 17:00 horas.

7.1.3. O agendamento deverá ser solicitado a Unidade de Segurança Cibernética da CODEVASF através do e-mail aa.gti.usc@codevasf.gov.br ou no telefone: (61) 2028-4765 ou (61) 2028-4364.

7.1.4. Nenhuma visita será realizada sem a confirmação de seu agendamento, por e-mail, por parte da Contratante.

8. PROPOSTA

8.1. As propostas de preços deverão conter no mínimo o seguinte:

a) Data, nome, endereço, e-mail, telefone, cidade, estado e país do licitante;

b) As especificações técnicas claras, completas e minuciosas dos fornecimentos ofertados, em conformidade com este Termo de Referência, podendo ser apresentada sob a forma de literatura, catálogo, desenhos e dados;

b1) Caso o licitante venha a fazer observações quanto aos requisitos técnicos exigidos nas especificações, o mesmo deverá explicitar, em sua proposta, uma lista de desvios em relação ao exigido, informando razões que a levaram a apresentar tais observações, fato este sujeito a aprovação pela CODEVASF;

c) Planilha de Proposta de Preços unitários e totais ofertados para os itens, devidamente preenchida, com clareza e sem rasuras, conforme modelo constante do Anexo V, que é parte integrante deste Termo de Referência;

d) Será de responsabilidade do licitante vencedor a prestação dos serviços desta contratação, cujos custos correram por sua exclusiva conta.

8.1.1. Nos preços unitários propostos, deverão estar incluídos todos os custos, seguros, transporte, mão-de-obra, leis sociais, encargos sociais, trabalhistas, previdenciárias, securitárias, tributos (ICMS, PIS, COFINS, IRRF, CSLL e IPI), e quaisquer encargos/taxas que incidam ou venham a incidir, direta ou indiretamente, nos fornecimentos objeto deste Termo de Referência. No caso de omissão, considerar-se-ão como inclusas nos preços.

8.1.2. Para efeito do disposto no subitem acima o licitante deverá considerar a tributação plena até o local da prestação de serviço, considerando que a CODEVASF não possui inscrição estadual, sendo considerada consumidora final. É de responsabilidade do licitando arcar com todos os tributos incidentes. A proposta deverá indicar em reais os preços dos materiais e serviços ofertados, com menção discriminada da referida tributação. A concorrente será responsável por quaisquer acréscimos que ocorrerem pela não observância desta particularidade.

8.1.3. Será considerada a melhor proposta, a que apresentar o MENOR PREÇO GLOBAL avaliado, POR ITEM, conforme critérios estabelecidos neste Termo de Referência.

8.1.4. Será desclassificada a proposta vencedora que:

a) tiver vícios insanáveis;
b) não obedecer às especificações técnicas contidas no Termo de Referência;
c) apresentar preços inexequíveis ou demonstrarem acima do preço máximo admitido para a contratação;

d) não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
e) apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável;

8.1.5. 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.

8.1.6. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

9. DOCUMENTAÇÃO DE HABILITAÇAO

9.1. Deverá ser apresentada em conformidade com as prescrições das leis que regem a matéria, de acordo com a previsão estabelecida no instrumento convocatório.

9.2. QUALIFICAÇÃO TÉCNICA

9.2.1. A licitante deve apresentar dois ou mais atestados de capacidade técnica fornecidos por pessoas jurídicas, sejam elas de direito público ou privado. Esses documentos devem ser lavrados em papel timbrado, contendo o endereço e o CNPJ da empresa. Os atestados devem demonstrar que a empresa participante executa (ou já executou) no período mínimo de 12 meses, de maneira satisfatória, serviços de testes de intrusão (Pentest) em aplicações e serviços.

9.2.2. Os documentos apresentados, emitidos em idioma estrangeiro, deverão ser apresentados devidamente traduzidos para a língua portuguesa, por tradutor juramentado e registrado no Cartório de Títulos e Documentos.

9.2.3. A CONTRATANTE poderá, a qualquer fase deste processo licitatório, promover diligências/visita técnica com vistas a esclarecer ou a complementar a instrução do processo, obrigando-se as licitantes a prestar todos os esclarecimentos necessários, inclusive poderá ser requerida cópia do contrato, nota(s) fiscal(is) ou qualquer outro documento que comprove inequivocamente que o serviço apresentado no(s) atestado(s) foi prestado.

9.2.4. É permitida ao licitante a soma de atestados para o atendimento das exigências, desde que todas em seu nome em relação ao objeto fornecido.

9.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

9.3.1. As licitantes deverão apresentar, na fase de habilitação, capital social mínimo de 10% (dez por cento) do valor orçado pela CODEVASF no item da licitação que concorrer, não sendo de forma acumulativa.

10. ORÇAMENTO DE REFERÊNCIA E DOTAÇÃO ORÇAMENTÁRIA

10.1. A Codevasf se propõe a pagar pelos fornecimentos, objeto desta licitação, o valor máximo global de R$ 120.000,00 (cento e vinte mil reais), conforme indicado no anexo Anexo II - Preços Máximos deste Termo de Referência.

10.2. As despesas previstas correrão à conta da classificação funcional programática 04.122.0032.2000.0001 – Administração da Unidade - Plano Orçamentário 0005 - Tecnologia da Informação e Modernização da Gestão

Organizacional, PTRES 172116, Categoria Econômica 3, Despesa Corrente, sob a gestão da Área Administração de Tecnologia.

11. PRAZOS DE EXECUÇÃO DOS SERVIÇOS E DE VIGÊNCIA DO CONTRATO

11.1. O prazo para execução do objeto deste TR é de 20 meses, a partir da data de emissão da Ordem de Serviço, podendo ser prorrogado, mediante manifestação expressa das partes.

11.2. O prazo máximo para emissão da Ordem de Serviço é de 2 meses, contados da data de assinatura do contrato.

11.3. O prazo para vigência do contrato, contado em meses, a partir da data de sua assinatura, compreende o prazo máximo para emissão da Ordem de Serviço, o prazo de execução do objeto informado acima, acrescido de mais 2 meses consecutivos para recebimento definitivo e expedição do Termo de Encerramento Físico dos fornecimentos e pagamento da Nota Fiscal caso haja pagamento pendente, perfazendo um prazo total de vigência de 24 meses.

11.4. No interesse de ambas as partes, o objeto do Contrato poderá ser prorrogado até o limite de 60 meses, nos termos da Lei nº 13.303/2016, Art. 71.

12. MODELO DE GESTÃO E CRITÉRIOS DE MEDIÇÃO

12.1. O serviço será demandado à CONTRATADA pela Equipe de gestão e fiscalização do contrato da CONTRATANTE.

12.2. O serviço será planejado e realizado após a emissão da Ordem de Serviço. A medição dos serviços ocorrerá conforme as entregas das fases previstas neste Termo de Referência, conforme tabela abaixo. Ressalta-se que a UST foi utilizada de forma arbitrária para mensurar as entregas, não sendo equivalente à hora/homem, mas sim representando a unidade de pagamento vinculada à conclusão de etapas específicas do projeto.

Tabela 3

Entregas	Quantidade (USTs)
1 - Fase de Planejamento	
Reunião Inicial	2
Entrega do plano de testes	4
2 - Fase de Descoberta e Ataque	
Execução da descoberta e exploração	16
Campanha de conscientização para empregados	6
Realização da apresentação técnica	4
Relatório dos testes	16
3 - Fase de Reteste	
Reexecução da descoberta e exploração	16
Relatório do reteste	16
4 - Fase Final	
Relatório técnico final dos resultados	10
Realização da apresentação técnica final dos resultados	10

Total:	100

12.3. Os custos decorrentes das correções das inconformidades de um produto/serviço apontadas pelo CONTRATANTE correrão por conta da CONTRATADA, exceto se a causa da inconformidade for de responsabilidade exclusiva do CONTRATANTE, devidamente comprovada.

12.4. Para efeito de medição, a CONTRATANTE acompanhará cada entrega realizada de cada fase pela CONTRATADA, a fim de avaliar os serviços prestados pela CONTRATADA.

12.5. Para execução dos serviços, será implementado o método de trabalho baseado no conceito de delegação de responsabilidade. Esse conceito define: o CONTRATANTE como responsável pela gestão, fiscalização e controle do contrato, bem como pela atestação da aderência aos padrões de qualidade exigidos dos serviços entregues; e a CONTRATADA como responsável pela execução dos serviços e gestão dos profissionais a seu cargo.

13. METODOLOGIA DE AVALIAÇÃO DA EXECUÇÃO DOS SERVIÇOS

13.1. O serviço de Pentest deverá ter acompanhamento completo durante toda a vigência do contrato, fiscalizando todos os prazos do cronograma do projeto, abrangendo também os relatórios.

13.2. Durante a execução dos testes, a contratada deverá manter canal de comunicação ativo (e-mail, telefone ou chat corporativo) para esclarecimentos ou autorização de testes, no horário e tempo de resposta definido (SLA) acordado no cronograma aprovado pela contratante.

13.3. Será feita a medição do tempo de entrega referente aos prazos constantes dos Requisitos de Prazos, item 1.7 do Anexo III deste Termo de Referência e principalmente após a elaboração do Plano de Execução. Conforme item 1.2

13.4. Será feita a medição da quantidade de ativos cobertos após a execução/reexecução do pentest para cada tipo de ativo, conforme item 1.3 do Anexo III deste Termo de Referência. Fórmula: Cobertura de Escopo do Pentest (%) = (Ativos Testados / Ativos no Plano de Execução) * 100, Mínimo: 97% para cada tipo de ativo, caso contrário será considerado como inexecução parcial.

14. FORMAS E CONDIÇÕES DE PAGAMENTO

14.1. Os pagamentos, objeto desta licitação, serão efetuados em reais, com base no preço unitário do serviço, efetivamente entregue, contra a apresentação das Notas Fiscais/Faturas devidamente atestadas pela Fiscalização da CODEVASF, conforme legislação vigente.

14.2. Os pagamentos serão efetuados em duas etapas, após a conclusão da Fase 2 e da Fase 4 (tabela 3), sendo a primeira paga no valor de 48 USTs e a segunda em 52 USTs após o termo de recebimento definitivo, correspondente aos serviços efetivamente entregues, executados e aceitos, e de conformidade ao discriminado na proposta da CONTRATADA, mediante apresentação das faturas/notas fiscais devidamente atestadas pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

14.3. Os serviços ora contratados serão cobrados por meio de faturas/notas fiscais emitidas pela CONTRATADA, referentes aos serviços prestados, deverão ser entregues na AA/GTI no mesmo período e após serem atestadas pela fiscalização, serão pagas em até 30 (trinta) dias.

14.4. O pagamento será efetuado por meio de ordem bancária, e creditado em qualquer entidade bancária indicada na proposta, devendo para isto, ficarem explicitados o nome do Banco, Agência, localidade e número da conta corrente em que deverá ser efetivado o crédito, após a aceitação e atesto das Notas Fiscais/Faturas.

14.5. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, bem como, Nota Fiscal/Fatura que possua valor divergente do estabelecido no contrato, ou mesmo, que apresente mês de referência ou prazo para pagamento inferior a 30 (trinta) dias corridos.

14.6. A emissão da Ordem Bancária será efetuada, somente após a Nota Fiscal/Fatura ser conferida, aceita e atestada por empregado responsável e ter sido verificada a regularidade da CONTRATADA, mediante consulta on-line ao Sistema Unificado de Cadastro de Fornecedores – SICAF e às demais Certidões (CNDT) para comprovação, dentre outras coisas, do devido recolhimento das contribuições sociais (FGTS e Previdência Social) e demais tributos estaduais e federais, conforme cada caso.

14.7. O valor do pagamento será calculado conforme a efetiva execução dos serviços dentro dos níveis requeridos, descontadas as glosas, consoante gradação estabelecida nos itens 13 e 16 deste Termo de Referência.

14.8. Os respectivos documentos de consulta ao SICAF e às demais Certidões do subitem anterior deverão ser anexados ao processo de pagamento.

14.9. É de inteira responsabilidade da CONTRATADA a entrega a CONTRATANTE dos documentos de cobrança, acompanhados dos seus respectivos anexos, de forma clara, objetiva e ordenada, que se não for atendido, implica desconsideração pela CONTRATANTE dos prazos estabelecidos para conferência e pagamento. A Nota Fiscal/Fatura deverá ser cadastrada pela CONTRATADA no site indicado pela CONTRATANTE – protocolo digital, mediante cadastro prévio de responsabilidade da CONTRATADA, após assinatura do contrato.

14.10. A Nota Fiscal/Fatura deverá informar o valor do Imposto sobre a Renda (IR) e das contribuições a serem retidas na operação, para fins de retenção na fonte, de acordo com o art. 2º, § 6º da IN/SRF n.º 1234/2012, ou informar a isenção, não incidência ou alíquota zero, e respectivo enquadramento legal, sob pena de retenção do imposto de renda e das contribuições sobre o valor total do documento fiscal, no percentual correspondente à natureza do bem.

14.11. Havendo erro na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida pelo Fiscal à CONTRATADA e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento se reiniciará após a regularização da situação ou reapresentação do documento fiscal, não acarretando qualquer ônus a CONTRATANTE.

14.12. Constatada a situação de irregularidade da CONTRATADA no SICAF, ela será notificada, por escrito, sem prejuízo do pagamento pelo objeto já executado, para, num prazo de 05 (cinco) dias úteis, regularizar tal situação ou, no mesmo prazo, apresentar defesa, sob pena de rescisão do Contrato.

14.13. O prazo para regularização ou encaminhamento de defesa de que trata o subitem anterior poderá ser prorrogado uma vez e por igual período, a critério da CONTRATANTE.

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

14.15. Persistindo a irregularidade, a Administração deverá adotar as medidas necessárias à rescisão contratual em execução, nos autos dos processos administrativos correspondentes, assegurada à CONTRATADA a ampla defesa.

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

14.17. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do órgão ou entidade contratante, não será rescindido o contrato em execução com empresa CONTRATADA no SICAF.

14.18. A critério da CONTRATANTE poderão ser utilizados os créditos existentes em favor da CONTRATADA para compensar quaisquer possíveis despesas resultantes de multas, indenizações, inadimplências contratuais e/ou outras de responsabilidade desta última.

14.19. À CODEVASF fica reservado o direito de não efetuar o pagamento se, durante a execução dos serviços, estes não estiverem em perfeitas condições, de acordo com as exigências contidas no Termo de Referência e seus anexos.

14.20. Para efeito de pagamento, considerar-se-á paga a fatura na data da emissão da Ordem Bancária.

14.21. No caso de eventual atraso no pagamento, e mediante pedido da CONTRATADA, o valor devido será atualizado financeiramente, desde a data a que o mesmo se referia até a data do efetivo pagamento, com base no último percentual divulgado do ICTI — Índice de Custos de Tecnologia da Informação, aplicando-se a seguinte fórmula:

AM = P x I, onde:
AM = Atualização Monetária (valor a ser adicionado na parcela atrasada)
P = Valor da Parcela a ser paga; e
I = Percentual de atualização monetária, assim apurado:
I = (1+im1/100)dx1/30 x (1+im2/100)dx2/30 x ... x (1+imn/100)dxn/30 – 1, onde:
i = Índice de Custos de Tecnologia da Informação — ICTI no mês “m”;
d = Número de dias em atraso no mês “m”;
m = Meses considerados para o cálculo da atualização monetária.

15. REAJUSTAMENTO DOS PREÇOS

15.1. Os valores do contrato permanecem fixos e sem reajustes durante um período de um ano, contado a partir da data da apresentação da proposta.

15.2. O objeto será contratado pelo valor proposto, sujeito a reajuste anual de acordo com o Índice de Custos de Tecnologia da Informação (ICTI), conforme estabelecido pela Portaria GM/MP nº 424, de 7 de dezembro de 2017, e mantido pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

15.3. Nos reajustes posteriores ao primeiro, o intervalo mínimo de um ano será calculado a partir dos efeitos financeiros do último reajuste.

15.4. Em caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA o valor calculado com base na última variação conhecida, liquidando a diferença correspondente assim que o índice definitivo for divulgado. A CONTRATADA é obrigada a apresentar uma memória de cálculo referente ao reajustamento dos preços do valor remanescente, sempre que isso ocorrer.

15.5. Se o índice estabelecido para o reajuste for extinto ou não puder mais ser utilizado, será adotado, em substituição, o índice determinado pela legislação então vigente.

15.6. Na falta de previsão legal para o índice substituto, as partes concordarão em escolher um novo índice oficial para o reajuste do preço do valor remanescente por meio de um termo aditivo.

15.7. De acordo com o artigo 136, §1°, da Lei 14.133/2021, registros que não caracterizam alteração do contrato podem ser realizados por simples apostilamento, dispensada a celebração de termo aditivo. Isso se aplica em situações como variação do valor contratual para reajuste ou repactuação de preços previstos no próprio contrato, atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento, alterações na razão ou denominação social do contratado, e empenho de dotações orçamentárias.

15.8. A seguir será apresentada a fórmula para o reajustamento do contrato, que poderá ser aplicada da seguinte maneira:

FÓRMULA DE REAJUSTAMENTO

$$R = V(\frac{I_1 - I_0}{I_0})$$

Onde:
"R" é o valor do reajuste procurado
"V" é o valor contratual a ser reajustado
"I1" é o índice correspondente ao mês do aniversário da Proposta
"I0" é o índice inicial correspondente à data de apresentação da Proposta

16. MULTAS

16.1. Nos casos de atrasos na prestação dos serviços do objeto contratado, por culpa exclusiva da CONTRATADA, cabe a aplicação de multa sobre o valor do contrato/ordem de serviço por dia, sem prejuízo das demais sanções previstas na legislação e no Regulamento Interno de Licitações e Contratos, conforme abaixo:

a) 0,2% (dois décimos por cento) do valor do contrato por dia de atraso nas entregas estipuladas no item 1.7.2., e seus subitens, do Anexo III especificações técnicas detalhadas deste Termo de Referência, até o máximo de 12% (doze por cento).
b) 1% (um por cento) do valor da garantia contratual por dia de atraso, no caso de atraso injustificado na entrega da garantia contratual, até o máximo de 20% (vinte por cento).

c) 0,2% (dois décimos por cento), calculada sobre o valor total da contratação, por dia de atraso no cumprimento de quaisquer obrigações previstas em contrato e não arroladas acima, até o limite de 6% (seis por cento).

16.2. Nos casos de inexecução total ou parcial do objeto, medida pelas fases da tabela 3, item 12.2, por culpa exclusiva da CONTRATADA, será cobrada multa baseada no valor do contrato/ordem de serviço, sem prejuízo das demais sanções previstas na legislação e no Regulamento Interno de Licitações e Contratos, conforme abaixo:

a) Até o máximo de 10% (dez por cento) do valor do contrato no caso de inexecução parcial do contrato/ordem de serviço conforme a Tabela 5;

b) Até o máximo de 10% (dez por cento) do valor do contrato no caso de descumprimento das obrigações contratuais descritas na Tabela 5;

c) 12% (doze por cento) do valor do contrato/ordem de serviço no caso de inexecução total.

Tabela 4 – Inadimplências e o respectivo grau de penalidade - inexecução parcial

Inadimplências	Grau de Penalidade	Percentual do valor do contrato
Execução parcial de até 80% do valor contratual	01	2%
Execução parcial de até 60% do valor contratual	02	4%
Execução parcial de até 40% do valor contratual	03	8%
Execução parcial de até 20% do valor contratual	04	10%

Tabela 5 – Descumprimento de obrigação contratual e a respectivo penalidade

Ocorrência	Cálculo da multa
Não atendimento às determinações estipuladas pela FISCALIZAÇÃO, no prazo por ela estabelecido, desde que seja comunicada à CONTRATADA, através de comunicação formal do fiscal.	R$ 100,00 por dia de atraso
Não apresentação de itens exigidos em cláusulas editalícias ou contratuais, dentro do prazo estabelecido.	R$ 500,00 por dia de atraso

16.3. Comprovando o impedimento ou reconhecida a força maior, devidamente justificados e aceitos pela FISCALIZAÇÃO, em relação a um dos eventos arrolados na Tabela 4, a CONTRATADA ficará isenta das penalidades mencionadas.

16.4. A multa será calculada na forma prevista no edital ou no contrato e não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 25% (vinte e cinco por cento) do valor do contrato licitado ou celebrado, conforme previsão do artigo 167 do RILC.

16.5. Ocorrida a inadimplência, a multa será aplicada pela CODEVASF, após regular processo administrativo, observando-se o seguinte:

a. A multa será descontada da garantia prestada pela CONTRATADA;

b. Caso o valor da multa seja de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente;

c. Caso o valor do faturamento seja insuficiente para cobrir a multa, a CONTRATADA será convocada para complementação do seu valor no prazo de 5 (cinco) dias a contar da data da convocação;

d. Não havendo qualquer importância a ser recebida pela CONTRATADA, esta será convocada a recolher à Gerência de Finanças da CODEVASF– AE/GFN o valor total da multa, no prazo de 5 (cinco) dias, contado a partir da data da comunicação.

16.6. O licitante vencedor terá um prazo inicialmente de 10 (dez) dias úteis para defesa prévia e, posteriormente, diante de uma eventual decisão que lhe tenha sido desfavorável, terá mais um prazo de 10 (dez) dias úteis, contado a partir da data de cientificação da aplicação da multa, para apresentar recurso à CODEVASF. Ouvida a fiscalização e acompanhamento do contrato, o recurso será encaminhado à Assessoria Jurídica da Superintendência Regional/Sede, que procederá ao seu exame.

16.7. Após o procedimento estabelecido no item anterior, o recurso será apreciado pela Diretoria Executiva da CODEVASF, que poderá dar provimento ou não ao recurso.

16.8. Em caso de provimento do recurso, a CODEVASF se reserva o direito de cobrar perdas e danos porventura cabíveis em razão do inadimplemento de outras obrigações, não constituindo a relevação novação contratual nem desistência dos direitos que lhe forem assegurados.

16.9. Caso a Diretoria Executiva não dê provimento ao recurso, não caberá novo recurso administrativo.

17. GARANTIA DE EXECUÇÃO

17.1. Como garantia para a completa execução das obrigações contratuais e da liquidação das multas convencionais, fica estipulada uma "Garantia de Execução" no montante de 5% (cinco por cento) do valor do contrato, que deverá ser entregue em até 10 (dez) dias úteis após a assinatura do instrumento, em espécie, Seguro Garantia emitida por seguradora autorizada pela SUSEP ou Fiança Bancária, a critério da CONTRATADA.

17.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,08% (oito centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autoriza a CODEVASF a promover a rescisão do contrato por descumprimento de suas cláusulas, conforme dispõe as condições contratuais.

17.3. A garantia a que se refere o subitem acima deverá ser entregue na Gerência de Tecnologia da Informação da Área de Administração e Tecnologia da CODEVASF.

17.4. A garantia na forma de Carta de Fiança Bancária ou seguro garantia deverão estar em vigor e cobertura até o final do prazo previsto para assinatura do Termo de Encerramento Definitivo do Contrato, devendo mantê-la atualizada durante toda a vigência do contrato.

17.5. Após a assinatura do Termo de Encerramento Físico do contrato, será devolvida a “Garantia de Execução”, uma vez verificada a perfeita execução do objeto contratual.

17.6. A garantia em espécie deverá ser depositada em instituição financeira oficial, credenciada pela CODEVASF, em conta remunerada que poderá ser movimentada somente por ordem da CODEVASF.

17.7. A não integralização da garantia representa inadimplência contratual, passível de aplicação de multas e de rescisão, na forma prevista nas cláusulas contratuais.

17.8. Por ocasião de eventuais aditamentos contratuais que promovam acréscimos ao valor contratado ou prorrogações de prazo contratual, a garantia prestada deverá ser reforçada e/ou renovada, de forma a manter a observância do disposto no caput desta cláusula, em compatibilidade com os novos valores e prazos pactuados.

17.9. Não haverá qualquer restituição de garantia em caso de dissolução contratual, na forma do disposto na cláusula de rescisão, hipótese em que a garantia reverterá e será apropriada pela CODEVASF.

17.10. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

a) Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
b) Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
c) Multas moratórias e punitivas aplicadas pela CODEVASF à CONTRATADA; e
d) Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

18. FISCALIZAÇÃO

18.1. A gestão do contrato, bem como a fiscalização da execução dos serviços será realizada pela CODEVASF, por técnicos designados, a quem compete verificar a CONTRATADA está executando os trabalhos, observando o contrato e os documentos que o integram.

18.2. A Fiscalização deverá verificar, periodicamente, no decorrer da execução do contrato, se a CONTRATADA mantém, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, comprovada mediante consulta ao SICAF, CADIN ou certidões comprobatórias.

18.3. A Fiscalização terá poderes para agir e decidir perante a CONTRATADA, inclusive rejeitando fornecimentos que estiverem em desacordo com o Contrato, com as Normas Técnicas vigentes relacionadas ao objeto deste Termo de Referência e com a melhor técnica consagrada pelo uso, obrigando-se desde já a CONTRATADA a assegurar e facilitar o acesso da Fiscalização, aos materiais, e a todos os elementos que forem necessários ao desempenho de sua missão.

18.4. A Fiscalização terá plenos poderes para sustar qualquer serviço que não esteja sendo executado dentro dos termos do contrato, dando conhecimento do fato à Gerência de Tecnologia da Informação da Área de Administração e Tecnologia, responsável pela execução do contrato.

18.5. Cabe à Fiscalização verificar a ocorrência de fatos para os quais haja sido estipulada qualquer penalidade contratual. A Fiscalização informará ao setor competente quanto ao fato, instruindo o seu relatório com os documentos necessários, e em caso de multa, a indicação do seu valor.

18.6. Das decisões da Fiscalização poderá a CONTRATADA recorrer à Gerência de Tecnologia da Informação da Área de Administração e Tecnologia da CODEVASF, responsável pelo acompanhamento do contrato, no prazo de 10 (dez) dias úteis da respectiva comunicação. Os recursos relativos a multas serão feitos na forma prevista na respectiva cláusula.

18.7. A ação e/ou omissão, total ou parcial, da Fiscalização não eximirá a CONTRATADA da integral responsabilidade pela execução do objeto deste contrato.

18.8. Fica assegurado aos técnicos da CODEVASF o direito de a seu exclusivo critério, acompanhar, fiscalizar e participar, total ou parcialmente, diretamente ou através de terceiros, da execução dos serviços prestados pelo licitante vencedor, com livre acesso ao local de trabalho para obtenção de quaisquer esclarecimentos julgados necessários à execução dos serviços.

18.9. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis

19. RECEBIMENTO DEFINITIVO DOS FORNECIMENTOS

19.1. Após o término dos serviços objeto deste TR, a CONTRATADA requererá à CODEVASF, através da Fiscalização, o seu recebimento provisório, que deverá ocorrer no prazo de 15 (quinze) dias da data da solicitação dos mesmos.

19.1.1. O recebimento definitivo do objeto, após a sua conclusão, obedecerá ao disposto no descrito abaixo:

a) Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita do contratado;

b) Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais.

b1) O contratado é obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

19.1.2. Na hipótese de o termo circunstanciado ou a verificação a que se refere este item não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados à Administração nos 15 (quinze) dias anteriores à exaustão dos mesmos.

19.1.3. Os ensaios, testes e demais provas exigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado.

19.1.4. A CODEVASF rejeitará, no todo ou em parte fornecimento executado em desacordo com o contrato.

19.2. Na hipótese da necessidade de correção, será estabelecido um prazo para que a CONTRATADA, às suas expensas, complemente, refaça ou substitua as entregas/serviços rejeitados.

19.3. A CONTRATADA entende e aceita que o pleno cumprimento do estipulado neste item é condicionante para:

a) Emissão, pela CODEVASF, do Atestado de Capacidade Técnica;
b) Emissão do Termo de Encerramento Físico (TEF); e
c) Liberação da Garantia de Execução (caução)

19.4. Aceitos e aprovados os fornecimentos, a CODEVASF emitirá o Termo de Encerramento Físico (TEF), que deverá ser assinado por representante autorizado da CONTRATADA, possibilitando a liberação da prestação de garantia.

19.5. A última fatura somente será encaminhada para pagamento após a emissão do Termo de Encerramento Físico de Contrato (TEF), que deverá ser anexado ao processo de liberação e pagamento.

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

20. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

20.1. O licitante vencedor deverá observar os seguintes critérios de sustentabilidade ambiental, no que couber, conforme a Instrução Normativa SLTI/MP nº 01/2010:

20.2. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

20.3. Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

20.4. Que os bens devam ser, preferencialmente, acondicionados em embalagem adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

20.5. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

20.6. O licitante vencedor deverá apresentar certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências supracitadas.

20.7. Em caso de inexistência de certificação que ateste a adequação, a CODEVASF poderá realizar diligências para verificar a adequação do produto às exigências deste TR, antes da assinatura do contrato, correndo as despesas por conta do licitante vencedor. Caso não se confirme a adequação do produto, a proposta vencedora será desclassificada.

20.8. Caso a CONTRATADA seja detentora da norma ISO 14000, poderá apresentar certificação que substitui as exigências do item 20.2 e deve apresentar a adoção das práticas previstas nas normas, bem como o desfazimento sustentável ou reciclagem dos bens que forem inservíveis para o processo de reutilização.

21. OBRIGAÇÕES DA CONTRATADA

21.1. A CONTRATADA deve cumprir integralmente todas as obrigações estabelecidas no Termo de Referência, incluindo prazos e condições, assumindo todos os riscos, responsabilidades e despesas necessários para a execução do objeto do contrato. Esse compromisso visa assegurar que o serviço seja realizado conforme as especificações definidas pela Contratante.

21.2. A CONTRATADA deve indicar formalmente um representante autorizado no prazo de cinco dias úteis após a assinatura do contrato. Esse representante será responsável por garantir a comunicação eficiente e imediata com a Contratante, facilitando o andamento das atividades e o cumprimento de quaisquer instruções adicionais.

21.3. A CONTRATADA deve atender prontamente a todas as orientações, exigências e solicitações feitas pela equipe de fiscalização do contrato, assegurando que todas as diretrizes estabelecidas sejam seguidas, visando ao melhor cumprimento das atividades contratadas.

21.4. A CONTRATADA assume total responsabilidade por quaisquer danos que sejam causados tanto à Contratante quanto a terceiros, decorrentes de ações ou omissões de seus representantes. Essa responsabilidade inclui a adoção de medidas corretivas e reparatórias, sempre que necessário.

21.5. A CONTRATADA deve permitir que a Contratante realize a fiscalização da execução do contrato em qualquer momento. Ela deve acatar prontamente as decisões de suspensão do fornecimento quando justificadas, para que se mantenham as condições adequadas de prestação dos serviços.

21.6. Durante a vigência do contrato, a CONTRATADA deve manter as condições de habilitação e qualificação apresentadas no momento da contratação, garantindo a continuidade da capacidade técnica e financeira necessária para a execução do objeto.

21.7. Em situações em que se exige uma equipe técnica especializada, a CONTRATADA deve manter profissionais qualificados e capacitados para o fornecimento adequado da solução de Tecnologia da Informação e Comunicação (TIC), assegurando a eficiência e eficácia da execução do serviço.

21.8. A CONTRATADA deve ceder todos os direitos de propriedade intelectual sobre produtos e documentos que forem gerados durante o contrato à Administração, de forma que a Contratante possa utilizar o resultado dos serviços prestados sem restrições futuras.

21.9. O contrato deve ser executado de acordo com as diretrizes e requisitos da Lei Geral de Proteção de Dados (LGPD), assegurando que as informações tratadas sejam manipuladas de maneira segura e que a privacidade dos dados seja preservada.

21.10. A CONTRATADA deve se abster de divulgar quaisquer informações sobre os serviços prestados sem a autorização prévia da Contratante, assegurando a confidencialidade de dados e informações estratégicas do processo.

21.11. A CONTRATADA não deve utilizar as informações fornecidas pela Contratante para fins diferentes dos que foram estabelecidos no contrato, a fim de proteger o sigilo das informações e evitar desvios de finalidade.

21.12. A CONTRATADA será responsável por quaisquer vícios ocultos ou danos que possam advir do uso do objeto, de acordo com o que está estipulado no Código de Defesa do Consumidor, assegurando a plena conformidade com a legislação de proteção ao consumidor.

21.13. Em casos de itens avariados ou defeituosos, a CONTRATADA é obrigada a realizar a substituição ou reparo, às suas próprias custas, conforme descrito no Termo de Referência, assegurando a qualidade e funcionalidade dos produtos e serviços prestados.

21.14. Caso ocorra algum imprevisto que cause atraso na entrega, a CONTRATADA deve comunicar à Contratante com pelo menos 24 horas de antecedência, detalhando as razões do atraso e as medidas que estão sendo adotadas para evitar prejuízos ao cronograma do projeto.

21.15. A CONTRATADA deve garantir o suporte às licenças de eventuais ferramentas utilizadas através do fabricante, que deve estar disponível para assistência via telefone e e-mail, permitindo a resolução de problemas técnicos e dúvidas operacionais.

21.16. Após cada visita técnica ou serviço realizado, a CONTRATADA deve apresentar um relatório detalhado contendo datas, descrição do serviço e as intervenções feitas, mantendo um histórico completo das operações realizadas no âmbito do contrato.

21.17. A CONTRATADA deve assumir total responsabilidade por todas as obrigações trabalhistas e previdenciárias de seus funcionários, evitando qualquer transferência de responsabilidades para a Contratante.

21.18. A CONTRATADA deve relatar prontamente qualquer irregularidade verificada durante a execução dos serviços à Contratante, permitindo que medidas corretivas sejam adotadas de forma tempestiva.

21.19. A CONTRATADA deve disponibilizar todas as informações e esclarecimentos solicitados pela Contratante para a supervisão e acompanhamento da execução do contrato, promovendo o controle administrativo.

22. OBRIGAÇÕES DA CODEVASF

22.1. Exigir da CONTRATADA o cumprimento integral deste Contrato.

22.2. Esclarecer as dúvidas que lhe sejam apresentadas pela CONTRATADA, através de correspondências protocoladas.

22.3. Fiscalizar e acompanhar a execução do objeto do contrato.

22.4. Expedir por escrito, as determinações e comunicações dirigidas a CONTRATADA, determinando as providências necessárias à correção das falhas observadas.

22.5. Determinar as datas e os horários para realização das atividades/tests, prevendo o mínimo de impacto nas atividades dos usuários.

22.6. Rejeitar todo e qualquer fornecimento inadequado, incompleto ou não especificado e estipular prazo para sua retificação.

22.7. Emitir parecer para liberação das faturas, e receber os fornecimentos/serviços contratados.

22.8. Efetuar o pagamento no prazo previsto no contrato.

23. GARANTIA DOS SERVIÇOS

23.1. A CONTRATADA deve garantir que o teste será feito de maneira segura, não disruptiva, e que não causará indisponibilidade ou prejuízo aos sistemas ou dados da CONTRATANTE.

23.2. A empresa CONTRATADA deve assinar um acordo de confidencialidade que impeça o uso, compartilhamento ou divulgação das informações acessadas durante o pentest.

23.3. A CONTRATADA deve garantir que as especificações técnicas do Anexo III deste Termo de Referência sejam cumpridas.

24. MATRIZ DE RISCOS

24.1. A matriz de risco está apresentada no Anexo IV (Matriz de Riscos) deste Termo de Referência com o objetivo de definir os riscos a que está exposta à execução do objeto, advindas de eventos supervenientes à contratação, dado relevante para sua identificação, prevenção e respectivas responsabilidades pela eventual ocorrência, bem como para o dimensionamento das propostas pelas licitantes.

24.2. A CONTRATADA não é responsável pelos riscos relacionados ao objeto do ajuste cuja responsabilidade na Matriz de Riscos seja da CODEVASF.

24.3. A CONTRATADA é integral e exclusivamente responsável por todos os riscos relacionados ao objeto do ajuste, inclusive, sem limitação, daqueles alocados para a CONTRATADA.

24.4. Constitui peça integrante do contrato a Matriz de Riscos, independentemente de transcrição no instrumento.

24.5. A CONTRATADA tem pleno conhecimento, quando da participação do processo licitatório, da natureza e extensão dos riscos por ela assumidos e deve levar tais riscos em consideração na formulação de sua proposta.

24.6. O termo risco no contrato é designado como um evento ou uma condição incerta que, se ocorrer, tem um efeito em pelo menos um objetivo do objeto contratual. O risco é o resultado da combinação entre probabilidade de ocorrência de determinado evento futuro e o impacto resultante caso ele ocorra. Esse conceito pode ser ainda mais específico ao se classificar o risco como a probabilidade de ocorrência de um determinado evento que gere impactos econômicos positivos ou negativos, bem como no prazo de execução do contrato.

24.7. Sempre que atendidas as condições do contrato e mantidas as disposições do contrato e da matriz de riscos, considera-se mantido seu equilíbrio econômico-financeiro.

24.8. A CONTRATADA somente poderá solicitar a recomposição do equilíbrio econômico-financeiro ou aditivo de prazo nas hipóteses excluídas de sua responsabilidade na matriz de riscos.

24.9. Os casos omissos na matriz de riscos serão objeto de análise acurada e criteriosa, lastreada em elementos técnicos, por intermédio de processo administrativo para apurar o caso concreto.

24.10. A referida matriz de riscos é parte integrante do contrato, pois tais obrigações são de resultado e devidamente delimitadas neste TR.

25. PROPRIEDADE INTELECTUAL

25.1. A CONTRATADA cederá à CONTRATANTE, a propriedade intelectual em caráter definitivo dos resultados produzidos em consequência desta licitação, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, código-fonte dos programas em qualquer mídia, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

25.2. A CONTRATADA fica proibida de veicular e comercializar os produtos gerados relativos ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da CONTRATANTE.

26. CONDIÇÕES GERAIS

26.1. Este Termo de Referência e seus anexos farão parte integrante do contrato a ser firmado com a CONTRATADA, independentemente de transcrições.

27. ANEXOS

27.1. São ainda, documentos integrantes deste Termo de Referência:

- Anexo I – Justificativas
- Anexo II – Planilhas de Quantidades e Preços
- Anexo III – Especificações Técnicas
- Anexo IV – Matriz de Riscos
- Anexo V – Proposta de Preço

Ministério da Integração e do Desenvolvimento Regional – MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ANEXO I – Justificativas

Finalidade: Este anexo tem por finalidade incluir exigências e particularidades em função da especificidade dos serviços a serem adquiridos, previstas no Termo de Referência.

Aprovação do Termo de Referência e Estudo Técnico Preliminar – ETP:
O Termo de Referência e o Estudo Técnico Preliminar foram aprovados por ato da autoridade competente, conforme consta no processo 59500.001857/2025-15-e, peça 88, e-DOC EDD2387D

Justificativas:

Da escolha da solução mais adequada ao atendimento da necessidade:
A escolha de uma empresa especializada em pentest baseia-se em cinco pilares técnicos essenciais para garantir a qualidade e efetividade dos serviços:
Abordagem Metodológica: A empresa deve seguir metodologias reconhecidas internacionalmente (PTES, OSSTMM, CWE Top 25, NIST SP 800-115 ou OWASP Top 10) e realizar testes de intrusão manuais, que são mais completos e personalizados do que apenas varreduras automatizadas.
Qualificação Técnica da Equipe: Os profissionais devem possuir certificações renomadas (OSCP, C|PENT, CompTIA Pentest+), além de experiência comprovada em projetos similares e conhecimento das tecnologias da organização. A equipe deve estar atualizada com as ferramentas e técnicas mais recentes.
Qualidade das Entregas: Os relatórios devem ser claros, bem estruturados e relevantes, contendo sumário executivo, metodologia, detalhamento com evidências, classificação de severidade, recomendações práticas e um plano de ação priorizado. A qualidade do relatório é crucial como produto final do pentest.
Confidencialidade e Segurança: É mandatório o compromisso com a confidencialidade das informações, com procedimentos robustos de proteção de dados confidenciais, incluindo acordos de confidencialidade e políticas de segurança internas, e, idealmente, certificações como SOC 2.
Suporte Pós-Pentest: A empresa deve oferecer suporte contínuo após os testes, com esclarecimentos, orientações para implementação de recomendações e verificação da eficácia das correções, garantindo a mitigação efetiva dos riscos.

Dos requisitos de aceitação e pontuação das propostas:
Será escolhida a proposta mais vantajosa para a administração pública cumprindo as especificações técnicas.

Do procedimento de pesquisa de preços realizado e dos critérios adotados para a seleção dos orçamentos formadores do valor estimado:
A pesquisa de preços foi realizada com base em contratações governamentais ocorridas entre outubro de 2024 e outubro de 2025, complementada por pesquisa de mercado junto a fornecedores e referências públicas disponíveis, garantindo maior precisão e atualidade dos valores obtidos. Todos os valores coletados foram consolidados na planilha de custos, a qual foi devidamente preenchida, encaminhada para análise pela Gerência de Custos (AG/GCT), e cujo parecer de custos consta no processo 59500.001857/2025-15-e, peça 83, eDOC 495BD405.

Dos critérios de sustentabilidade ambiental:
A inclusão dos critérios de sustentabilidade ambiental previstos nos itens 20.1 a 20.8 do Termo de Referência justifica-se pela necessidade de atender à Instrução Normativa SLTI/MP nº 01/2010 e aos princípios da Lei nº 14.133/2021, garantindo que os bens adquiridos apresentem menor impacto ambiental, utilizem materiais recicláveis ou atóxicos, sigam padrões reconhecidos de certificação (como ABNT, INMETRO e RoHS) e adotem práticas de responsabilidade ambiental em toda a cadeia de fornecimento. Tais exigências asseguram maior segurança química, redução de resíduos, adequação ao ciclo de vida sustentável e mitigação de riscos à Administração, além de promover economicidade e conformidade com as boas práticas de desenvolvimento sustentável recomendadas pelos órgãos de controle.

Das exigências habilitatórias indispensáveis à garantia do cumprimento das obrigações:

São necessárias as comprovações de qualificação de experiencia e econômico financeira, conforme Resolução DEX nº 821/2023.

Da necessidade da contratação:
A contratação deste Termo de Referência é fundamental para assegurar a avaliação contínua da postura de segurança da organização, por meio da realização de testes de intrusão (pentest) que identifiquem vulnerabilidades técnicas em sistemas e aplicações críticas. Além disso, contempla a execução de campanhas de conscientização voltadas aos usuários visando à mitigação de riscos decorrentes de falhas humanas e ao fortalecimento da cultura organizacional de segurança da informação, em consonância com os princípios da eficiência, transparência e interesse público previstos na Lei nº 13.303/2016.

Alinhamento Estratégico:

• A presente demanda encontra guarita nos seguintes instrumentos quanto ao seu alinhamento estratégico:

1. No Planejamento Estratégico Institucional - PEI 2025-2030, nas perspectivas: Gestão e Governança: OE2 – Promover a Modernização Tecnológica e a Transformação Digital e OE3 – Fortalecer a Governança, Gestão de Riscos e Integridade.

2. No Plano Estratégico de Tecnologia da Informação - PETI 2023-2027, Objetivo Estratégico de TI: - OETI01 – Aprimorar a Segurança da Informação, na iniciativa IETI 03 – Prover a automação dos recursos de segurança da informação (firewalls, Anti-Spam, Anti-Ransoware, IPS/ IDS etc) em todas as unidades; - OETI06 - Padronizar e fortalecer a infraestrutura de TI, na iniciativa; IETI 17 - Fornecer equipamentos (hardwares e softwares).

3. Após análise da AA/GTI/UPC, foi constatado que o projeto não consta no rol de ações previsto no PDTI 2023-2027, no entanto, o projeto foi priorizado pelo Comitê de Governança Digital durante sua 1ª Reunião Extraordinária, realizada em 27 de novembro de 2024 (A5DDE73C), conforme solicitado na Nota de Encaminhamento nº 01 (B23EC3DF).

Da escolha de item único:
A consolidação desses objetos em um item único justifica-se pela sinergia entre as ações, uma vez que ambas, pentest e campanha de conscientização, possuem como finalidade a elevação do nível de maturidade em segurança cibernética, atuando de forma complementar: os pentests identificam vulnerabilidades técnicas, enquanto as campanhas reduzem riscos associados ao fator humano.
Adicionalmente, destaca-se que o Termo de Referência adota a métrica de Unidades de Serviço Técnico (USTs) para a mensuração dos serviços, o que permite o adequado acompanhamento, controle e pagamento proporcional às entregas em um item único.
Outro ponto importante é que a adoção por item único facilita a fiscalização e gestão contratual o que é importante frente ao número de servidores disponíveis para consecução dessas duas atividades. Desta forma, o agrupamento de elementos que compõem a mesma solução compõe a melhor estratégia da Administração, quando a adjudicação de itens isolados onera “o trabalho da administração pública, sob o ponto de vista do emprego de recursos humanos e da dificuldade de controle, colocando em risco a economia de escala e a celeridade processual”, vide o ACÓRDÃO Nº5301/2013 – TCU – 2ª Câmara.

Da adoção pelo uso do Pregão Eletrônico: A modalidade de Pregão Eletrônico foi adotada em razão do objeto da contratação ser bem comum, cujos padrões de desempenho e qualidade foram objetivamente definidos nas especificações deste Termo de Referência, por meio de padrões usuais de mercado, em conformidade com o disposto no art. 32, inciso IV e § 3º da Lei nº 13.303/2016.
O objeto desta contratação é considerado bem/serviço comum, pois tem padrões desempenho e qualidade objetivamente definidos neste Termo de Referência, por meio de especificações usuais no mercado.

Justificativa da adoção do valor estimado público: Conforme Acórdão nº 1502/2018 – Plenário TCU, nas licitações realizadas pelas empresas estatais, sempre que o orçamento de referência for utilizado como critério de aceitabilidade das propostas, sua divulgação no edital é obrigatória, e não facultativa, em observância ao princípio constitucional da publicidade e, ainda, por não haver no art. 34 da Lei nº 13.303/2016 (Lei das Estatais) proibição absoluta à revelação do orçamento.

Critério de Julgamento: Menor preço, de acordo com o Art. 67 do Regulamento Interno de Licitações e Contratos da Codevasf. Visa obter a proposta mais vantajosa para a administração, desde que atendidos os parâmetros mínimos de desempenho, de qualidade, as especificações técnicas e requisitos de habilitação estabelecidos no Edital e seus anexos, a fim de proporcionar um julgamento igualitário entre os licitantes, sendo definido o critério de julgamento por item.

Dos requisitos de Qualificação Técnica: Os itens, que compõe a Qualificação Técnica (Habilitação) do presente TR, foram selecionados conforme a complexidade dos serviços a serem contratados.

Dos requisitos de Qualificação Econômico-Financeira:
A qualificação econômico-financeira foi estabelecida com base na experiência da PR/SLC em procedimentos anteriores, adoutou-se a exigência de Capital Social conforme o edital.

Da não exclusividade e/ou cota reservada para ME/EPP: microempresas e empresas de pequeno porte:
Não – Devido ao valor do item ser superior a R$ 80.000,00, não é possível reservar cota de até 25% ou aplicar exclusividade para ME/EPP, pois a adoção do benefício implicaria restrição de competitividade e risco à adequada execução do objeto.

Permite Participação de Consórcios:
Não – por se tratar de fornecimento de serviços comuns, a logística necessária para cumprimento do objeto não exige o envolvimento de empresas com diferentes especialidades, não sendo consequentemente pertinente a formação de consórcios com intuito de reforçar a capacidade técnica e financeira do licitante. As empresas isoladas podem perfeitamente conseguir preencher os requisitos necessários para tal.

Permissão para Participação de Sociedades Cooperativas:
Não será permitida a participação de pessoas jurídicas organizadas sob a forma de Cooperativas uma vez que as especificidades do objeto e da prestação de serviço/operações/atividades exige uma gestão operacional centralizada e não concede autonomia dos cooperados, conforme exigido pela IN MPOG 05/2017.

Permite Subcontratação:
Não será aceito a subcontratação devido à impossibilidade de parcelamento do item contratado.

Garantia Contratual/Garantia de Execução (Caução): Devido ao valor elevado do objeto licitado e o tempo de garantia do serviço a ser fornecido, que será de 24 meses, faz-se necessária a caução de 5% (cinco por cento) do valor do contrato.

Ministério da Integração e do Desenvolvimento Regional – MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ANEXO II

PLANILHA DE QUANTIDADES E PREÇOS ORÇADOS

Ministério da Integração e do Desenvolvimento Regional – MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

Item	Descrição/ Especificação	Catmat/ Catser	Unidade	Qtd	Valor máximo unitário	Valor máximo total
1	Serviços de Consultoria em Segurança de Tecnologia da Informação e Comunicação (TIC) - Análise de vulnerabilidades e testes de intrusão (pentest).	27340	Unidade de Serviço Técnico	100	R$ 1.200,00	R$ 120.000,00
					Valor Total:	R$ 120.000,00

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ANEXO III – ESPECIFICAÇÕES TÉCNICAS

OBJETIVO

Este anexo descreve as especificações técnicas para o fornecimento de serviços especializados de teste de invasão (pentest) e da campanha de conscientização para usuários. Abrangendo avaliação de vulnerabilidades, execução de testes em aplicações, estações de trabalho, infraestrutura de rede, servidores, roteadores, switches, Wi-Fi e outros dispositivos. A elaboração de relatórios técnicos e executivos contendo evidências, recomendações e plano de mitigação. Para a CODEVASF em Brasília – DF.

Especificações detalhadas do item

REQUISITOS MÍNIMOS NECESSÁRIOS

1.1. **Escopo do Pentest**

1.1.1. A CONTRATANTE fornecerá o escopo do Pentest à CONTRATADA. Esta retornará com o documento Plano de Execução, contendo o cronograma das atividades, o qual deverá ser aprovado ou reprovado pelo CONTRATANTE.

1.1.1.1. O escopo consiste em um ambiente de até 2679 ativos, contabilizados entre estações de trabalho, servidores, aplicações, roteadores, switches, rede Wi-Fi e outros dispositivos.

Tipos de Ativos	Quantidade de Ativos
Estações de trabalho (desktops e notebooks)	2200
Servidores on-premises (virtualizados e físicos)	200
Aplicações Web	130
Roteadores	19
Switches	92
Rede Wi-Fi	18
Outros Dispositivos	20
Total	2679

1.1.1.2. O Plano de Execução deverá contemplar, obrigatoriamente, a cobertura mínima de 80% dos ativos de cada tipo, conforme quantidades apresentadas no item 1.1.1.1. salvo impedimentos devidamente justificados no Relatório Técnico.

1.1.2. Os tipos de teste poderão ser: black box, gray box ou white box, conforme solicitação da CONTRATANTE. Além de registrar os testes positivos de exploração, deve-se documentar os casos de testes mal sucedidos, com vistas a evidenciar a eficácia dos controles de segurança

existentes.

1.1.3. Os testes que demandarem execução presencial (in loco) deverão ser realizados exclusivamente na sede da CODEVASF, em Brasília/DF.

1.1.4. O pentest terá as seguintes fases:

1.1.4.1. Fase de Planejamento: composto por Reunião Inicial entre CONTRATANTE E CONTRATADA, para detalhamento e entendimento da demanda, com vistas a subsidiar a elaboração e formalização do Plano de Execução por parte da CONTRATADA. Detalhamento no item 1.2 deste TR.

1.1.4.2. Fase de Descoberta e Ataque: composto pela execução da descoberta e exploração de vulnerabilidades; elaboração de relatório técnico contendo achados, evidências (logs, capturas de tela, provas de conceito), classificação de risco (criticidade), impacto potencial e recomendações práticas para correção e redução do risco; realização de sessão de entrega com a equipe técnica e partes interessadas para exposição dos resultados, priorização das ações corretivas, esclarecimento de dúvidas e definição dos próximos passos. Detalhamento nos itens 1.3 deste TR.

1.1.4.3. Fase de Reteste: reexecução das rotinas de varredura, enumeração e tentativas de exploração sobre os pontos corrigidos, utilizando os mesmos métodos e escopo aplicados originalmente, para validar a eficácia das medidas implementadas; realização de sessão de entrega com a equipe técnica e partes interessadas para exposição dos resultados (vulnerabilidades remediadas ou persistentes), priorização das ações corretivas, esclarecimento de dúvidas e, se necessário, recomendações adicionais ou encaminhamento para novo ciclo de correção. Detalhamento nos itens 1.4 deste TR.

1.1.4.4. Fase Final: consolida todos os trabalhos realizados ao longo do pentest, formalizando os resultados, comunicando-os às partes interessadas e promovendo ações de fortalecimento da postura de segurança humana na organização. Nesta etapa são entregues documentos finais, realizado um seminário de apresentação. Detalhamento nos itens 1.5 e 1.6 deste TR.

1.2. Planejamento

1.2.1. Reunião inicial

1.2.1.1. Na fase de Planejamento do Pentest, a CONTRATADA e a CONTRATANTE detalham o escopo do teste, o cronograma macro das atividades a serem realizadas, para elaboração do plano de execução.

1.2.1.1.1. Nesta fase serão definidos os canais de comunicação entre CONTRATADA e CONTRATANTE durante a realização do teste.

1.2.2. Entrega do plano de execução

1.2.2.1. O plano deve ser formalizado pela CONTRATADA, em documento contendo, pelo menos:

1.2.2.1.1. Descrição e tamanho do escopo do teste por tipo de ativos;

1.2.2.1.2. O sistema ou ativo de tecnologia a ser testado;

1.2.2.1.3. A modalidade de pentest a ser realizado: Black Box, Gray Box ou White Box;

1.2.2.1.4. A forma de realização do pentest: externo ou interno;

1.2.2.1.5. Uma vez definido o escopo, o prazo e o cronograma de execução das atividades, o início da execução dos serviços deverá ocorrer na data e prazo previstos.

1.2.2.1.6. Cronograma das atividades;

1.2.2.1.7. Ferramentas, sistemas e metodologias a serem utilizados na execução das atividades, assim como credenciais necessárias e outros recursos para bem executar o teste solicitado;

1.2.2.1.8. Formas de contato;

1.2.2.1.9. Contatos para emergência;

1.2.2.1.10. Mapeamento de responsabilidades.

1.2.2.2. O cronograma deve contemplar a data de entrega do Plano de Execução, do Relatório do Pentest e da apresentação técnica do Relatório, além das demais atividades operacionais relativas ao teste.

1.2.2.3. O documento citado no item 1.2.2.1 deve ser entregue à CONTRATANTE em até 10 dias úteis após a emissão da OS (Ordem de Serviço) para avaliação e aprovação.

1.2.2.4. No caso de testes remotos, a CONTRATADA deverá fornecer previamente o(s) endereço(s) de IP de onde partirão as ações referentes aos testes de segurança, para possibilitar que a CONTRATANTE diferencie as atividades relacionadas aos serviços contratados de eventuais atividades suspeitas/maliciosas reais em curso.

1.2.2.5. O plano de execução não pode conter processos, técnicas ou procedimentos que estejam fora da área de especialização ou nível de competência do analista que o executará.

1.3. Descoberta e Ataque

1.3.1. Execução da descoberta e exploração

1.3.1.1. Descoberta: contempla a realização de coleta passiva e ativa de informações para cada tipo de ativo, servindo como insumo para os relatórios e a elaboração dos testes e execução da análise das vulnerabilidades existentes.

1.3.1.2. Deve ser utilizada, no mínimo, 01 (uma) solução e/ou ferramenta de análise de vulnerabilidades juntamente com técnicas e ações manuais de levantamento de informações e de análise de vulnerabilidade.

1.3.1.3. A(s) solução(ões) e/ou ferramenta(s) utilizada(s) deve(m) contemplar, no mínimo, as seguintes características:

1.3.1.3.1. Realizar o levantamento e a análise de vulnerabilidades sem a necessidade de instalação de agentes na infraestrutura tecnológica da CONTRATANTE;

1.3.1.3.2. Suportar o armazenamento seguro de credenciais de acesso fornecidas pela CONTRATANTE, para realização de varreduras autenticadas do tipo gray box e white box em ativos, sistemas ou serviços.

1.3.1.3.3. Permitir a parametrização da carga gerada pelas ações, de forma a evitar que a ferramenta cause sobrecarga de recursos avaliados.

1.3.1.3.4. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste Termo de Referência e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas pela CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável do CONTRATANTE.

1.3.1.3.5. Suportar ou ser compatível com, pelo menos, identificação por CVE.

1.3.1.3.6. Apresentar a descrição das vulnerabilidades encontradas, contendo, pelo menos, as seguintes informações:

1.3.1.3.6.1. Nome;
1.3.1.3.6.2. Número MITRE, NVD, SANS, CVE ou CVSS, se houver algum deles;
1.3.1.3.6.3. Nível/categorização de risco (exemplos: baixo, médio, alto, crítico);
1.3.1.3.6.4. Descrição;
1.3.1.3.6.5. Formas de exploração;
1.3.1.3.6.6. Recomendação de correção;
1.3.1.3.6.7. Link da correção/patch, se aplicável;

1.3.1.3.7. Apresentar evidências de ativos não encontrados ou não vulneráveis por meio de evidências como:

1.3.1.3.7.1. Falhas nas varreduras;
1.3.1.3.7.2. Resultado de varreduras esperados versus obtidos;
1.3.1.3.7.3. Lista de ativos não analisados;

1.3.1.4. Ataque: execução de atividades com o intuito de explorar as vulnerabilidades encontradas nos ativos definidos no escopo, registrando os resultados obtidos. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste

estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas no CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável do CONTRATANTE.

1.3.1.4.1. O pentest deve identificar as seguintes fragilidades, quando aplicável:

1.3.1.4.1.1. Acesso não autorizado e/ou privilegiado a informações, serviços, sistemas e ativos;
1.3.1.4.1.2. Defacement;
1.3.1.4.1.3. Escalação horizontal e/ou vertical de privilégios;
1.3.1.4.1.4. Negação de serviço, distribuído ou não, volumétrico, esgotamento de recursos e na camada de aplicação;
1.3.1.4.1.5. Ataques de amplificação;
1.3.1.4.1.6. Exploração das top 10 vulnerabilidades listadas pela OWASP;
1.3.1.4.1.7. Vazamento e/ou roubo de informações;
1.3.1.4.1.8. Execução não autorizada de comandos;
1.3.1.4.1.9. Inclusão remota de código;

1.3.1.5. A depender do tipo de Pentest a ser realizado, a CONTRATADA não precisará informar à CONTRATANTE o início de cada fase do teste, devendo tal condição ser prevista no documento de Plano de Execução.

1.3.1.6. A lista de testes citada acima é exemplificativa, podendo outros tipos de testes serem realizados, desde que planejados pelo CONTRATANTE e a CONTRATADA, antes ou durante a execução do teste inicial.

1.3.1.7. Ao ser encontrada ou explorada uma vulnerabilidade considerada crítica/grave, a CONTRATADA deverá informá-la à CONTRATANTE imediatamente, relatando qual, quando e como a vulnerabilidade foi encontrada e explorada, as medidas necessárias para correção da vulnerabilidade e, quando possível, ações de contorno para evitar a ocorrência de ataque real até que a correção vulnerabilidade seja implementada;

1.3.1.7.1. Mesmo que seja informado à CONTRATANTE, tal vulnerabilidade, a forma de exploração e respectiva correção, deverão constar no relatório, elaborado ao final do Pentest.

1.3.1.8. Qualquer atividade com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada antes de sua execução, haja vista a necessidade de manutenção da integridade, confidencialidade e disponibilidade do ambiente tecnológico da CONTRATANTE.

1.3.1.8.1. Os testes poderão ser interrompidos por solicitação expressa do CONTRATANTE a qualquer instante.

1.3.1.9. O Pentest deve ser realizado conforme as práticas e técnicas especificadas pelos padrões internacionais, além de outros apresentados pela empresa CONTRATADA, caso haja, em seu portfólio, normativos que, comprovadamente, complementam os já citados.

1.3.1.10. A execução dos testes deve envolver técnicas e procedimentos dentre os listados a seguir, além de outros não listados e que sejam aplicáveis ao escopo:

1.3.1.10.1. Uso de códigos maliciosos – essa ação deve ter a autorização prévia do CONTRATANTE, solicitada antes ou durante os testes;

1.3.1.10.2. Negação de serviço – ataques DoS e DDoS, se necessários, deverão ser realizados mediante expressa autorização da CONTRATANTE, que definirá o período e condições para execução dos testes.

1.3.1.10.3. Resistência a spoofing;

1.3.1.10.4. Implantação de coletores de pacotes (packet sniffers), controles remotos e outras ferramentas de monitoração, quando e onde couber;

1.3.1.10.5. Testes remotos de quebra de senhas via dicionário, força bruta ou man-in-the-middle;

1.3.1.10.6. Busca por vulnerabilidades quanto à personificação de máquinas confiadas (trusted hosts) e eventuais anomalias de roteamento;

1.3.1.10.7. Vulnerabilidades quanto à adulteração do DNS (DNS spoofing);

1.3.1.10.8. Deverão ser analisadas vulnerabilidades associadas a diversos serviços como Web servers, Application Servers, FTP Servers, Mail Servers, DNS Server, SSH, dentre outros;

1.3.1.10.9. Escalação de privilégios em Active Directory;

1.3.1.10.10. Movimentação lateral em ambiente de Active Directory;

1.3.1.10.11. Demais métodos e técnicas listados pelo MITRE ATT&CK;

1.3.1.10.12. Demais métodos e técnicas listados pelo OWASP WSTG para ambientes web.

1.3.1.11. Para fins de testes a partir da rede interna, a CONTRATANTE poderá oferecer à CONTRATADAS equipamentos com imagem padrão para o acesso ao ambiente tecnológico da CODEVASF.

1.3.2. **Campanha de conscientização para empregados**

1.3.2.1. Esta fase contempla a execução de teste de phishing e engenharia social, como também a divulgação da conscientização para os empregados.

1.3.2.2. Escopo

1.3.2.2.1. Palestra presencial na sede da codevasf com transmissão para as Superintendências da Codevasf, linguagem acessível, material de apoio. Carga horária de 4 (quatro horas), e emissão de certificado de participação.

1.3.2.2.1.1. Não haverá um número especificado de participantes, deverá ser ministrada para o alcance completo da codevasf.

1.3.2.2.2. Montagem de Materiais de Conscientização: cartilhas, vídeos, infográficos, e-mails periódicos.

1.3.2.2.3. Simulações de Engenharia Social:

1.3.2.2.3.1. Phishing: envio de e-mails falsos simulados, coleta de métricas (abertura, clique, fornecimento de credenciais).

1.3.2.2.3.2. Vishing: ligações simuladas tentando obter dados, avaliando resistência.

1.3.2.2.4. Relatórios:

1.3.2.2.4.1. De desempenho da simulação.

1.3.2.2.4.2. Relatório da campanha com análise, métricas e recomendações.

1.3.2.3. A empresa CONTRATADA deve prover equipe técnica qualificada (especialista em SI, instrutores, analistas).

1.3.2.4. Conteúdo customizado à realidade do órgão.

1.3.2.5. Condução segura das simulações (sem coleta de dados reais, relatórios anonimizados).

1.3.2.6. Conformidade com LGPD e normas internas.

1.3.3. **Relatórios**

1.3.3.1. **Relatório dos testes**

1.3.3.1.1. Após finalizadas todas as atividades referentes a descoberta e ataque, a CONTRATADA deve elaborar, apresentar e entregar à CONTRATANTE o Relatório técnico do Pentest, conforme estabelecido no cronograma do Plano de Execução.

1.3.3.1.2. O relatório do pentest deverá ser um documento técnico contendo o detalhamento do planejamento do teste e de todas as ações executadas, com recomendações de ações para corrigir as vulnerabilidades encontradas, além das evidências (captura de tela ou vídeos ilustrando a exploração), devendo incluir eventuais casos mal sucedidos. O relatório deve conter, no mínimo, as seguintes informações:

1.3.3.1.2.1. Objetivos e escopo do teste;

1.3.3.1.2.2. Janela de tempo dos testes de segurança realizados;

1.3.3.1.2.3. Informações obtidas por meio do levantamento passivo e ativo de informações;

1.3.3.1.2.4. Metodologia de análise de vulnerabilidades;

1.3.3.1.2.5. Lista de vulnerabilidades encontradas, contendo, no mínimo as informações citadas no item 1.3.3.6;

1.3.3.1.2.6. Lista de ativos enumerados vulneráveis e não vulneráveis;

1.3.3.1.2.7. Informações referentes aos ataques realizados, destacando a vulnerabilidade explorada, método e vetores de exploração, além do resultado do ataque;

1.3.3.1.2.8. Apresentação das evidências de exploração/ataque apuradas;

1.3.3.1.2.9. Informações acessadas oriundas do sucesso do ataque;

1.3.3.1.2.10. Informações dos ataques mal sucedidos, devido aos controles de segurança da informação existentes, apresentando evidências.

1.3.3.1.2.11. Recomendações e controles de segurança necessários para correção das vulnerabilidades;

1.3.3.1.2.12. Caso existente, indicação da solução de contorno para evitar a exploração de vulnerabilidade até que ela seja corrigida.

1.3.3.1.2.13. Referências técnicas e ferramentas utilizadas;

1.3.3.1.2.14. Todas as ações de levantamento de informações, análise de vulnerabilidades e de ataques deverão ser ordenadas sequencialmente, citando o comando correspondente e data/hora da execução.

1.3.3.1.2.15. As evidências deverão referenciar a linha de comando que as originaram.

1.3.3.1.3. O relatório da campanha de conscientização para empregados deverá ser um documento técnico contendo o detalhamento do planejamento do ataque e da campanha de conscientização, de todas as ações executadas desta etapa. O relatório deve conter, no mínimo, as seguintes informações:

1.3.3.1.3.1. Objetivos e escopo do teste;

1.3.3.1.3.2. Janela de tempo dos testes e da campanha realizados;

1.3.3.1.3.3. Informações obtidas por meio do levantamento passivo e ativo de informações;

1.3.3.1.3.4. Metodologia do ataque e da campanha;

1.3.3.1.3.5. Estatísticas da campanha de conscientização (lista não exaustiva):

1.3.3.1.3.5.1. Percentual de abertura do e-mail;

1.3.3.1.3.5.2. Percentual de cliques no link de phishing;

1.3.3.1.3.5.3. Percentual de fornecimento de credenciais;

1.3.3.1.3.5.4. Setores da empresa mais vulneráveis;

1.3.3.1.4. O relatório deverá ser assinado pela equipe ou responsável técnico diretamente envolvido com a realização dos testes.

1.3.3.1.4.1. O relatório deverá incluir uma Seção Executiva, contendo o resumo gerencial do teste e de seus resultados. Nesta Seção, deverá haver a indicação de possíveis riscos decorrentes da exploração das vulnerabilidades encontradas, além dos testes executados que não foram bem sucedidos devido à eficácia dos controles existentes, bem como as ações prioritárias para o tratamento dos riscos identificados.

1.3.4. **Realização da apresentação técnica**

1.3.4.1. A apresentação do relatório deverá ser realizada em reunião própria, a ser realizada nas dependências da CONTRATANTE ou de forma remota, em data a ser agendada entre CONTRATANTE e CONTRATADA.

1.3.4.1.1. A CONTRATANTE poderá, mediante prévio agendamento com a CONTRATADA, solicitar apresentação presencial, se entender necessária.

1.3.4.2. O relatório deve ser entregue nos formatos .docx ou em .odt, e também em .pdf, na língua português do Brasil, em endereço de correio eletrônico a ser definido no Plano de Execução.

1.4. **Fase de Reteste**

1.4.1. **Reexecução da descoberta e exploração**

1.4.1.1. Descoberta: contempla a realização de coleta passiva e ativa de informações para cada tipo de ativo necessárias para a elaboração do reteste e reexecução de ações para levantamento e análise das vulnerabilidades já detectadas.

1.4.1.2. O reteste será executado uma única vez para todos os ativos do escopo planejado, sendo este solicitado após as correções ou prazo informado no planejamento.

1.4.1.2.1. Para vulnerabilidades classificadas como críticas e altas, a CONTRATANTE poderá solicitar o reteste antes do prazo informado.

1.4.1.3. Deve ser utilizada, no mínimo, 01 (uma) solução e/ou ferramenta de análise de vulnerabilidades juntamente com técnicas e ações manuais de levantamento de informações e de análise de vulnerabilidade.

1.4.1.4. A(s) solução(ões) e/ou ferramenta(s) utilizada(s) deve(m) contemplar, no mínimo, as seguintes características:

1.4.1.4.1. Realizar o levantamento e a análise de vulnerabilidades sem a necessidade de instalação de agentes na infraestrutura tecnológica da CONTRATANTE;

1.4.1.4.2. Suportar o armazenamento seguro de credenciais de acesso fornecidas pela CONTRATANTE, para realização de varreduras autenticadas do tipo gray box e white box em ativos, sistemas ou serviços.

1.4.1.4.3. Permitir a parametrização da carga gerada pelas ações, de forma a evitar que a ferramenta cause sobrecarga de recursos avaliados.

1.4.1.4.4. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste Termo de Referência e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas pela CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável do CONTRATANTE.

1.4.1.4.5. Suportar ou ser compatível com, pelo menos, identificação por CVE.

1.4.1.4.6. Apresentar a descrição das vulnerabilidades encontradas, contendo, pelo menos, as seguintes informações:

1.4.1.4.6.1. Nome;
1.4.1.4.6.2. Número MITRE, NVD, SANS, CVE ou CVSS, se houver algum deles;
1.4.1.4.6.3. Nível/categorização de risco (exemplos: baixo, médio, alto, crítico);
1.4.1.4.6.4. Descrição;
1.4.1.4.6.5. Formas de exploração;
1.4.1.4.6.6. Recomendação de correção;
1.4.1.4.6.7. Link da correção/patch, se aplicável;

1.4.1.4.7. Apresentar evidências de ativos não vulneráveis, se encontrados, por meio de evidências como:

1.4.1.4.7.1. Falhas nas varreduras;
1.4.1.4.7.2. Resultado de varreduras esperados versus obtidos;
1.4.1.4.7.3. Lista de ativos não analisados;

1.4.1.5. Ataque: execução de atividades com o intuito de explorar as vulnerabilidades encontradas nos ativos definidos no escopo, registrando os resultados obtidos. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste

estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas na CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável do CONTRATANTE.

1.4.1.5.1. O pentest deve identificar as seguintes fragilidades, quando aplicável:

1.4.1.5.1.1. Acesso não autorizado e/ou privilegiado a informações, serviços, sistemas e ativos;
1.4.1.5.1.2. Defacement;
1.4.1.5.1.3. Escalação horizontal e/ou vertical de privilégios;
1.4.1.5.1.4. Negação de serviço, distribuído ou não, volumétrico, esgotamento de recursos e na camada de aplicação;
1.4.1.5.1.5. Ataques de amplificação;
1.4.1.5.1.6. Exploração das top 10 vulnerabilidades listadas pela OWASP;
1.4.1.5.1.7. Vazamento e/ou roubo de informações;
1.4.1.5.1.8. Execução não autorizada de comandos;
1.4.1.5.1.9. Inclusão remota de código;

1.4.1.6. A depender do tipo de Pentest a ser realizado, a CONTRATADA não precisará informar à CONTRATANTE o início de cada fase do teste, devendo tal condição ser prevista no documento de Plano de Execução.

1.4.1.7. A lista de testes citada acima é exemplificativa, podendo outros tipos de testes serem realizados, desde que planejados pelo CONTRATANTE e a CONTRATADA, antes ou durante a execução do teste inicial.

1.4.1.8. Ao ser encontrada ou explorada uma vulnerabilidade considerada crítica/grave, a CONTRATADA deverá informá-la à CONTRATANTE imediatamente, relatando qual, quando e como a vulnerabilidade foi encontrada e explorada, as medidas necessárias para correção da vulnerabilidade e, quando possível, ações de contorno para evitar a ocorrência de ataque real até que a correção vulnerabilidade seja implementada;

1.4.1.8.1. Mesmo que seja informado à CONTRATANTE, tal vulnerabilidade, a forma de exploração e respectiva correção, deverão constar no relatório, elaborado ao final do Pentest.

1.4.1.9. Qualquer atividade com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada antes de sua execução, haja vista a necessidade de manutenção da integridade, confidencialidade e disponibilidade do ambiente tecnológico da CONTRATANTE.

1.4.1.9.1. Os testes poderão ser interrompidos por solicitação expressa do CONTRATANTE a qualquer instante.

1.4.1.10. O Pentest deve ser realizado conforme as práticas e técnicas especificadas pelos padrões internacionais, além de outros apresentados pela empresa CONTRATADA, caso haja, em seu portfólio, normativos que, comprovadamente, complementam os já citados.

1.4.1.11. A execução dos testes deve envolver técnicas e procedimentos dentre os listados a seguir, além de outros não listados e que sejam aplicáveis ao escopo:

1.4.1.11.1. Uso de códigos maliciosos – essa ação deve ter a autorização prévia do CONTRATANTE, solicitada antes ou durante os testes;

1.4.1.11.2. Negação de serviço – ataques DoS e DDoS, se necessários, deverão ser realizados mediante expressa autorização da CONTRATANTE, que definirá o período e condições para execução dos testes.

1.4.1.11.3. Resistência a spoofing;

1.4.1.11.4. Implantação de coletores de pacotes (packet sniffers), controles remotos e outras ferramentas de monitoração, quando e onde couber;

1.4.1.11.5. Testes remotos de quebra de senhas via dicionário, força bruta ou man-in-the-middle;

1.4.1.11.6. Busca por vulnerabilidades quanto à personificação de máquinas confiadas (trusted hosts) e eventuais anomalias de roteamento;

1.4.1.11.7. Vulnerabilidades quanto à adulteração do DNS (DNS spoofing);

1.4.1.11.8. Deverão ser analisadas vulnerabilidades associadas a diversos serviços como Web servers, Application Servers, FTP Servers, Mail Servers, DNS Server, SSH, dentre outros;

1.4.1.11.9. Escalação de privilégios em Active Directory;

1.4.1.11.10. Movimentação lateral em ambiente de Active Directory;

1.4.1.11.11. Demais métodos e técnicas listados pelo MITRE ATT&CK;

1.4.1.11.12. Demais métodos e técnicas listados pelo OWASP WSTG para ambientes web.

1.4.1.12. Para fins de testes a partir da rede interna, a CONTRATANTE poderá oferecer à CONTRATADA, equipamentos com imagem padrão para o acesso ao ambiente tecnológico da CODEVASF.

1.4.2. Relatórios

1.4.2.1. Relatório do reteste

1.4.2.1.1. Após finalizadas todas as atividades referentes a descoberta e ataque, a CONTRATADA deve elaborar, apresentar e entregar à CONTRATANTE o Relatório técnico do Pentest, conforme estabelecido no cronograma do Plano de Execução.

1.4.2.1.2. O relatório do pentest deverá ser um documento técnico contendo o detalhamento do planejamento do reteste e de todas as ações executadas, com recomendações de ações para corrigir as vulnerabilidades encontradas, além das evidências (captura de tela ou vídeos ilustrando a exploração), devendo incluir eventuais casos mal sucedidos. O relatório deve conter, no mínimo, as seguintes informações:

1.4.2.1.2.1. Objetivos e escopo do reteste;

1.4.2.1.2.2. Janela de tempo dos testes de segurança realizados;

1.4.2.1.2.3. Informações obtidas por meio do levantamento passivo e ativo de informações;

1.4.2.1.2.4. Metodologia de análise de vulnerabilidades;

1.4.2.1.2.5. Lista de vulnerabilidades encontradas, contendo, no mínimo as informações citadas no item 1.3.3.6;

1.4.2.1.2.6. Lista de ativos enumerados vulneráveis e não vulneráveis;

1.4.2.1.2.7. Informações referentes aos ataques realizados, destacando a vulnerabilidade explorada, método e vetores de exploração, além do resultado do ataque;

1.4.2.1.2.8. Apresentação das evidências de exploração/ataque apuradas;

1.4.2.1.2.9. Informações acessadas oriundas do sucesso do ataque;

1.4.2.1.2.10. Informações dos ataques mal sucedidos, devido aos controles de segurança da informação existentes, apresentando evidências;

1.4.2.1.2.11. Recomendações e controles de segurança necessários para correção das vulnerabilidades;

1.4.2.1.2.12. Caso existente, indicação da solução de contorno para evitar a exploração de vulnerabilidade até que ela seja corrigida;

1.4.2.1.2.13. Referências técnicas e ferramentas utilizadas;

1.4.2.1.2.14. Todas as ações de levantamento de informações, análise de vulnerabilidades e de ataques deverão ser ordenadas sequencialmente, citando o comando correspondente e data/hora da execução; e

1.4.2.1.2.15. As evidências deverão referenciar a linha de comando que as originaram.

1.4.2.1.3. O relatório deverá incluir uma Seção Executiva, contendo o resumo gerencial do teste e de seus resultados. Nesta Seção, deverá haver a indicação de possíveis riscos decorrentes da exploração das vulnerabilidades encontradas, além dos testes executados que não foram bem sucedidos devido à eficácia dos controles existentes, bem como as ações prioritárias para o tratamento dos riscos identificados.

1.5. Fase Final

1.5.1. Relatório técnico final dos resultados

1.5.1.1. Além das informações já citadas em 1.3.3 e 1.4.2.

1.5.1.2. O relatório final deve conter métricas da diferença entre o teste o reteste dos seguintes itens.

1.5.1.2.1. O relatório do pentest, deve conter a diferença dos resultados entre o teste e o reteste.

1.5.1.2.2. O relatório da campanha de conscientização.

1.5.2. Realização da apresentação técnica final dos resultados

1.5.2.1. A apresentação do relatório deverá ser realizada em reunião própria, a ser realizada nas dependências da CONTRATANTE ou de forma remota, em data a ser agendada entre CONTRATANTE e CONTRATADA.

1.5.2.1.1. A CONTRATANTE poderá, mediante prévio agendamento com a CONTRATADA, solicitar apresentação presencial, se entender necessária.

1.5.2.2. O relatório deve ser entregue nos formatos .docx ou em .odt, e também em .pdf, na língua portuguêsdo Brasil, em endereço de correio eletrônico a ser definido no Plano de Execução.

1.6. Outras Definições

1.6.1. Todos os relatórios, rotinas e scripts desenvolvidos exclusivamente para a execução dos testes de segurança deverão ser fornecidos pela CONTRATADA à CONTRATANTE, os quais passarão a ser de propriedade intelectual da CONTRATANTE ao final da execução da demanda.

1.6.1.1. Excluem-se as rotinas, ferramentas e scripts que sejam licenciados e parte de soluções licenciadas utilizadas pela CONTRATADA na realização dos testes.

1.6.2. A CONTRATADA não poderá alterar e/ou apagar quaisquer informações e dados aos quais tiver acesso durante a realização dos testes de segurança executados, bem como não poderá alterar a configuração de ativos, serviços e sistemas que fizerem parte do escopo do teste.

1.6.3. É de responsabilidade da CONTRATADA o provimento de softwares e respectivas licenças, além de hardwares, necessários à realização das atividades vinculadas à execução do trabalho.

1.6.4. As atividades descritas neste Termo de Referência não poderão se resumir apenas ao uso de ferramentas automatizadas, sendo obrigatória a atuação de equipe especializada na realização de análises e testes dessa natureza, devendo esta realizar análises qualitativas que extrapolam os possíveis relatórios gerados pelas ferramentas.

1.6.5. Para toda vulnerabilidade encontrada, a CONTRATADA deverá descrevê-la de forma detalhada, contendo, sempre que possível, as TTPs (Tactics, Techniques, and Procedures) da base de conhecimento MITRE ATT&CK, CVE e CVSS, assim como as ações para sua correção e possíveis formas de detecção.

1.6.5.1. Caso seja necessário acesso às configurações dos ativos de tecnologia ou ao código fonte para propor as soluções de correção, a CONTRATADA deverá justificar a necessidade, ficando a cargo da CONTRATANTE a decisão pela liberação do acesso.

1.6.6. A CONTRATADA, em conjunto com a CONTRATANTE, deverá estabelecer plano de comunicação entre envolvidos e conhecedores dos testes. O plano deve especificar, pelo menos, para quem, como e quando a comunicação ocorrerá, contemplando casos em que a equipe de teste comprometa o ativo e/ou sistema, se alguma falha de segurança for descoberta ou se a realização do teste causar problemas inesperados para a CONTRATANTE.

1.6.7. A CONTRATADA deverá propor padrão ou framework utilizado amplamente no mercado para registrar os resultados dos testes de segurança e detalhar as evidências no relatório emitido a cada Pentest, no intuito de servir como referência técnica, durante processo de auditoria interna e externa.

1.6.8. A CONTRATADA deverá, ao final dos testes de segurança, remover os códigos de teste e arquivos desnecessários, contendo ou não informações sigilosas, incluindo as contas criadas para realizar os serviços.

1.6.8.1. Quando a CONTRATADA não possuir autonomia suficiente para execução das ações listadas no item acima, deverá informar à equipe técnica da CONTRATANTE quais contas, arquivos e rotinas utilizadas para os testes deverão ser removidos ou desabilitados no ambiente tecnológico.

1.6.9. A CONTRATADA deve apresentar um cronograma com todas as etapas, atividades e seus respectivos tempos para execução.

1.6.10. Para auxílio das atividades, poderão, a critério da CONTRATANTE, ser solicitados à CONTRATADA reuniões e relatórios de acompanhamento periódico do plano de execução.

1.6.11. Os testes a serem executados deverão utilizar como referência ao menos uma das seguintes metodologias: PTES, OSSTMM, OWASP, NIST 800-115, ISSAF e PTF ou, ainda, outro framework, de acordo com a necessidade.

1.6.11.1. A utilização de frameworks diferentes dos citados deverá ser submetida à aprovação da CONTRATANTE para a inclusão no escopo de teste.

1.7. **Requisitos de Prazo**

1.7.1. O tempo estimado para cada teste deve considerar as atividades entre: planejamento, varreduras, mapeamentos, testes e análise e elaboração de relatório.

1.7.2. Prazos máximos de execução para cada atividade:

1.7.2.1. Planejamento: até 10 dias úteis, a partir da emissão da Ordem de Serviço. Entregável: Plano de Execução.

1.7.2.2. Descoberta e Ataque: observar o cronograma previamente definido no Plano de Execução.

1.7.2.3. Relatório: após a conclusão das atividades anteriores ao relatório, a CONTRATADA tem até 5 dias úteis para a elaboração e entrega do Relatório Técnico do Pentest. Entregável: Relatório.

Ministério da Integração e do Desenvolvimento Regional
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba

Versão 9.0

MATRIZ DE RISCOS

PROCESSO:	59500.001857/2025-15-e
OBJETO DA CONTRATAÇÃO:	Contratação de Serviços Especializados para execução de Testes de Intrusão (PENTEST).
OBJETIVO DA CONTRATAÇÃO:	Identificar falhas de segurança em sistemas, aplicações e infraestrutura de TI, permitindo a mitigação de riscos cibernéticos, a proteção de dados pessoais e a conformidade com a Lei Geral de Proteção de Dados (LGPD), Plano Nacional de Segurança da Informação (PNSI), normas e frameworks internacionais de segurança da informação.
LOCAL DE EXECUÇÃO:	Brasília/DF
ÁREA/UNIDADE SUPRIDORA:	AA/GTI/USC
ÁREA/UNIDADE DEMANDANTE:	AR/SE

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento
RC004	Gestão contratual	Falta de planejamento ou gestão ineficaz do projeto	Poderá acontecer o comprometimento do cronograma e da execução do contrato	Atraso no cronograma de implantação	Contratante	3- Média	2- Pequeno		0	
RC007	Gestão contratual	Dependência de terceiros ou atrasos no fornecimento	Poderá ocorrer atraso no início da prestação de serviços contratados	Atraso na disponibilização da solução	Compartilhado	3- Média	2- Pequeno		0	
RC008	Gestão contratual	Dimensionamento incorreto da capacidade do fornecedor	Poderá acontecer a contratação de serviços que não atendam à necessidade do requisitante	Atraso na prestação do serviço ou atendimento parcial	Compartilhado	2- Baixa	2- Pequeno		0	
RC009	Gestão contratual	Inadimplência contratual ou cláusulas mal definidas	Poderá ocorrer diversas alterações no andamento da execução	Não execução do contrato ou execução parcial	Contratada	2- Baixa	3- Moderado		0	
RC010	Gestão contratual	Falta de monitoramento e controle de prazos	Poderá acontecer o comprometimento do cronograma e da execução do contrato	Atraso no conograma da implantação.	Contratante	2- Baixa	3- Moderado		0	
RC011	Gestão contratual	Mudanças constantes de escopo ou má gestão financeira	Poderá acontecer elevação dos preços praticados pela contratada ou perda de autonomia da contratante em executar serviços essenciais de TI	Aumento no custo do projeto	Contratante	2- Baixa	2- Pequeno		0	

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento
RC012	Gestão contratual	Falha em sistemas principais ou falta de plano de contingência	Poderá ocorrer indisponibilidade de serviços críticos que possuam dependências	Serviços críticos inoperantes	Compartilhado	3- Média	4- Grande		0	
RC013	Gestão contratual	Falhas em backups ou erros operacionais humanos	Poderá ocorrer danos ou perda de informações	Dados sensíveis excluídos	Compartilhado	3- Média	3- Moderado		0	
RC014	Gestão contratual	Escopo mal definido ou comunicação ineficiente entre as partes	Poderá ocorrer adaptações no escopo para execução de testes	Não atendimento ao escopo esperado	Compartilhado	3- Média	3- Moderado		0	
RC015	Gestão contratual	Falhas de segurança ou má configuração de acessos	Poderá ocorrer exposição de informações sensíveis	Vazamento de dados corporativos	Compartilhado	3- Média	4- Grande		0	
RC016	Gestão contratual	Fornecedor sem capacidade técnica ou financeira	Poderá ser selecionado um fornecedor inadequado ou sem aptidão técnica	Não execução do contrato ou execução parcial	Compartilhado	1- Muito baixa	2- Pequeno	Risco Moderado	0	
RC017	Gestão contratual	Falta de plano de resposta a incidentes ou de contingência	Poderá ocorrer acesso indevido ao sistema	Prejuízo financeiro e de pessoal para reestabelecer serviços e reparar danos	Contratada	3- Média	2- Pequeno		0	
RC018	Gestão contratual	Não conformidade com normas legais ou regulamentares	Poderá ocorrer procedimentos em que a empresa considera legal pode ser visto como irregular pela fiscalização ou por auditorias.	Violação de leis	Contratada	3- Média	2- Pequeno		0	

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

* Ocultar as linhas que não forem utilizadas e formatar a altura das linhas.

COORDENADOR DO PROJETO OBJETO DA CONTRATAÇÃO - DEMANDANTE			
No	André Luis Gomes Moreira	**Lotação:**	AA/GTI/USC

ANALISTAS RESPONSÁVEIS PELO MAPEAMENTO DOS RISCOS DA CONTRATAÇÃO - DEMANDANTE			
No	Rui Ramos de Andrade Lima Bisneto	**Lotação:**	AA/GTI/USC
No		**Lotação:**	
No		**Lotação:**	
No		**Lotação:**	
No		**Lotação:**	

LOCAL/DATA:	02/10/2025

Obs.: Em 16 de dezembro de 2024, foi aprovado o "Plano de Gerenciamento de Riscos em Contratações e Doações da Codevasf", que contempla o Modelo de Elaboração do Mapa e Matriz de Contratações, por meio da Deliberação nº 57 de dezembro de 2024 (processo nº 59500.003411/2024-44-e). O Plano atende à recomendação nº 4 do Relatório de Auditoria nº 902916-Controladoria-Geral da União - CGU (Processo nº 59500.002345/2022-23-e) que em 31 de dezembro de 2024

Ministério da Integração e do Desenvolvimento Regional – MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ANEXO V

PROPOSTA DE PREÇO

DADOS DA PROPONENTE

Razão Social: _____
CNPJ: _____ Inscrição Estadual: _____
Representante(s) legal(is) com poder para assinar contrato _____
CPF: _____ RG: _____ Órgão Expedidor _____ UF ___
Endereço completo: _____
Cidade: _____ CEP: _____ Telefone: (___) _____
E-mail: _____ Contato: _____
Validade da Proposta (mínimo 60 dias): _____

Item	Descrição/ Especificação	Catmat/ Catser	Unidade	Qtd	Valor máximo unitário	Valor máximo total
1	Serviços de Consultoria em Segurança de Tecnologia da Informação e Comunicação (TIC) - Análise de vulnerabilidades e testes de intrusão (pentest).	27340	Unidade de Serviço Técnico	100		
					Valor Total:	

Declaramos que nos preços propostos estão incluídos todos os custos e despesas de qualquer natureza, incidentes sobre os objetos desta proposta.

Declaramos total conhecimento e concordância dos termos do edital do pregão e dos seus anexos. Em anexo documentação complementar com descrição da solução e equipamentos que a compõem.

Cidade (UF), _____ de _____ de 202__.

_____

Ministério da Integração e do Desenvolvimento Regional – MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

Nome Completo Responsável CPF