BANCO CENTRAL DO BRASIL - BRASÍLIA

Termo de Referência 42/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
42/2026	179087-BANCO CENTRAL DO BRASIL - BRASÍLIA	FELIPE KENZO SHIRAISHI	13/11/2026 14:54 (v 0.28)

Status

DISPONIBILIZADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
V - prestação de serviços, inclusive os técnico-profissionais especializados/Serviço continuado sem dedicação exclusiva de mão de obra	45/2026	305279

1. Condições Gerais da Contratação

1.1. Contratação de Serviços Especializados em Gestão de Vulnerabilidades, Testes de Invasão, Inspeção de Código-Fonte, Modelagem de Ameaças e Mensuração de Riscos Cibernéticos, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Item	Especificação	CATSER	Métrica ou Unidade de Medida	Quantidade	Valor Unitário	Valor Total
1	Serviços Especializados em Gestão de Vulnerabilidades, Testes de Invasão, Inspeção de Código-Fonte, Modelagem de Ameaças e Mensuração de Riscos Cibernéticos, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.	27022	Meses	48	R$ 251.903,52	R$ 12.091.369,03

1.2. O serviço especializado especificado como item 1 a ser contratado é composto pela relação de subitens apresentados a seguir:

Subitem	Descrição	Quantidade	Métrica ou Unidades	Valor Unitário	Valor Total
1	Serviço contínuo de gestão de vulnerabilidades	48	meses	R$ 51.857,98	R$ 2.489.183,10
2	Serviço contínuo de testes de invasão (pentesting)	48	meses	R$ 76.718,64	R$ 3.682.494,85
3	Serviço contínuo de inspeção de código fonte	48	meses	R$ 50.680,55	R$ 2.432.666,20

4	Banco de horas de testes de invasão	4000	horas	R$ 263,59	R$ 1.054.358,69
5	Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos	48	meses	R$ 50.680,55	R$ 2.432.666,20

Classificação do objeto quanto à heterogeneidade ou complexidade

1.3. Os serviços objeto desta contratação são caracterizados como **comuns** nos termos do artigo 6, inciso XXI, da Lei nº 14.133/2021 pelos serviços enumerados apresentarem padrões de desempenho e qualidade objetivamente mensuráveis, independentemente de sua complexidade técnica. Conforme apurado a partir do Estudo Técnico Preliminar, há atendimento de 3 critérios: (1) os serviços listados possuem escopo mensurável, conforme a delimitação orientada a projetos, sistemas e notificações de vulnerabilidades; (2) os serviços apresentam parâmetros claros de entrega, orientados a relatórios, prazos, quantidade mensal estimada, indicadores de esforços e requisitos técnicos; (3) conforme pesquisa de mercado realizada, há ampla oferta de fornecedores prestando tais serviços, o que evidencia padronização e maturidade do serviço.

Classificação do objeto quanto ao modelo de execução

1.4. O serviço é enquadrado como continuado tendo em vista que as atividades sendo contratadas constituem necessidades permanentes, cíclicas e essenciais à manutenção da segurança cibernética do BCB, sendo inadequada a execução por escopos isolados, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar;

Prazo de vigência

1.5. O prazo de vigência da contratação é de **4 anos** contados a partir da data da sua assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

1.6. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

Caracterização do objeto como não sobreposição à atividade fim do Banco Central

1.7. O objeto da presente contratação não se sobrepõe à atividade fim do banco central de regular o sistema financeiro nacional e executar a política monetária do país, mas auxilia a atividade meio de contribuir com a resiliência dos sistemas de TIC mantidos pelo Banco Central ao contribuir com a revisão de controles e estado da segurança dos sistemas mantidos pela instituição. Dessa forma, o objeto desta contratação não se trata de um objeto passível de restrição de contratação de acordo com o art. 48 da Lei 14.133 de 2021.

2. Fundamentação e Descrição da Necessidade

2.1. A presente contratação tem por finalidade solucionar limitações operacionais identificadas no Estudo Técnico Preliminar (ETP), referentes à execução dos processos de gestão de vulnerabilidades, testes de invasão, inspeção de códigofonte e modelagem de ameaças/mensuração de riscos. Tais atividades integram diretamente as atribuições da área de segurança cibernética do Banco Central do Brasil (BCB) e são indispensáveis para garantir a continuidade, confiabilidade e resiliência dos serviços essenciais prestados à sociedade e ao Sistema Financeiro Nacional (SFN).

2.2. O ETP demonstra que o BCB opera um ambiente tecnológico complexo, composto por mais de 9.000 ativos de TIC, mais de 6.000 softwares distintos e mais de 1.600 projetos de código-fonte, resultando em mais de 1.200 imagens de container em produção, o que caracteriza um cenário de grande heterogeneidade e elevada superfície de ataque. Esse contexto, aliado ao volume crescente de vulnerabilidades publicadas no cenário global, com projeção de 80.000 CVEs até 2030, equivalendo a aproximadamente 225 vulnerabilidades diárias, impõe à instituição a necessidade de manter processos contínuos, tempestivos e especializados de detecção, análise e mitigação de riscos cibernéticos.

2.3. Para mensurar o esforço requerido, o ETP aplicou fatores de atenuação baseados na realidade do BCB (percentual de CVEs críticas, softwares efetivamente utilizados e existência de ferramentas internas), chegando a um esforço diário estimado entre 5 e 8 vulnerabilidades relevantes até 2030, demonstrando a necessidade concreta de capacidade operacional especializada e contínua para o gerenciamento adequado desses eventos.

2.4. Os impactos da insuficiência de capacidade operacional interna foram igualmente quantificados: a área de segurança enfrenta atualmente limitações por competir com outras atribuições funcionais e por possuir número reduzido de servidores, o que compromete a

tempestividade das análises e cria risco de janelas de exposição, afetando diretamente a resiliência cibernética institucional e podendo gerar atrasos na entrega de serviços mediados por TIC, críticos à atuação do BCB, como pagamentos, liquidação, supervisão e processamento sistêmico.

2.5. Com base nesses riscos, o ETP identificou 5 (cinco) necessidades institucionais essenciais:

2.5.1. suporte contínuo em gestão de vulnerabilidades;
2.5.2. suporte em testes de invasão (pentests);
2.5.3. suporte em inspeção de códigofonte;
2.5.4. suporte em modelagem de ameaças e mensuração de riscos;
2.5.5. elasticidade operacional para pentests conforme variação de demanda.

2.6. Essas necessidades foram caracterizadas detalhadamente no documento, demonstrando vínculo direto com a sobrecarga atual e com a incapacidade de atendimento tempestivo utilizando exclusivamente recursos internos.

2.7. A definição do quantitativo necessário de serviços também foi fundamentada com base em estimativas operacionais apresentadas no ETP. O estudo estabeleceu a necessidade de 5 (cinco) profissionais, conforme o volume histórico e projetado de demandas:

2.7.1. gestão de vulnerabilidades: capacidade de tratar, pelo menos, 8 vulnerabilidades diárias, com uma média de 1 hora de trabalho por vulnerabilidade endereçada;
2.7.2. testes de invasão: demanda mínima de 2 testes mensais, com esforço estimado de 160 horas de trabalho por teste, em média;
2.7.3. inspeção manual de códigofonte: 1 inspeção por mês com esforço estimado de 160 horas de trabalho por inspeção, em média;
2.7.4. modelagem de ameaças/mensuração de riscos: 8 avaliações por ano, com esforço estimado de 240 horas de trabalho por avaliação

2.8. Esses quantitativos resultaram diretamente do diagnóstico de demanda histórica, projeção de carga para 2030 e capacidade interna disponível, atendendo ao requisito de proporcionalidade e precisão na definição de volumes contratados.

2.9. Além disso, o ETP demonstrou que outras alternativas foram avaliadas, como contratação por escopo e execução integral por esforço interno, mas ambas foram consideradas inadequadas por não atenderem requisitos de continuidade, sinergia técnica, tempestividade, escalabilidade e retenção de conhecimento. O modelo por escopo foi formalmente classificado como inviável devido à impossibilidade de se ajustar às variações imprevisíveis da demanda, à perda de sinergia entre processos correlatos e ao aumento de retrabalho operacional.

2.10. Quanto à vantajosidade econômica, o estudo concluiu que o custo total de propriedade (TCO) da solução contínua é metade do custo econômico estimado para execução integral via esforço interno, considerando o custo médio por servidor e a projeção de redução do quadro funcional. A comparação demonstra que a contratação representa clara economia de recursos públicos e assegura maior eficiência operacional, além de permitir continuidade e previsibilidade ao longo dos anos.

2.11. A contratação também está alinhada aos objetivos estratégicos OE1 (governança e gestão de recursos de TIC) e OE7 (segurança cibernética e privacidade digital) do PDTIC 20202025, reforçando seu caráter essencial para o cumprimento das funções institucionais do BCB, incluindo a preservação da infraestrutura crítica nacional conforme o Decreto nº 11.200/2022.

2.12. Diante de todas essas evidências, volume crescente e mensurável de vulnerabilidades, complexidade e extensão do ambiente tecnológico do BCB, quantificação precisa do esforço requerido, insuficiência comprovada da força de trabalho interna, riscos operacionais específicos, impacto direto sobre serviços críticos, inviabilidade técnica de alternativas e vantajosidade econômica demonstrada, a contratação dos serviços especializados é não apenas necessária, mas indispensável para garantir a segurança, a continuidade e a resiliência da atuação institucional do Banco Central do Brasil.

2.13. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

I) ID PCA no PNCP: 00038166000105-0-000007/2026;
II) Data de publicação no PNCP: 09/05/2025;
III) Id do item no PCA: 934;
IV) Classe/Grupo: 162 – Serviços de gerenciamento em tecnologia da informação e comunicação (TIC);
V) Identificador da Futura Contratação: 179087-45/2026;

2.14. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024-2027 (SGD/MGI nº 4.248/2024), o Plano Estratégico Institucional do Banco Central (PEI-BCB) e em consonância com o Plano Diretor de Tecnologia da Informação (PDTI) 2026-2029 do Banco Central do Brasil, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**

PEI-BCB nº 3	Aumentar a eficiência do sistema financeiro e das infraestruturas digitais públicas para promover bem-estar econômico e acesso a serviços financeiros adequados.
SGD/MGI nº4	Ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

ALINHAMENTO AO PDTI 2026-2029			
ID	**Ação do PDTI**	**ID**	**Meta do PDTI associada**
A	Aprimorar os processos para que as iniciativas de TI sejam priorizadas e executadas conforme estratégia do BCB.	**OE1**	Aprimorar a governança, os processos internos e a gestão dos recursos de TIC
A	Aprimorar a resiliência cibernética no BCB	**OE 7**	Promover segurança cibernética e privacidade digital
D	Identificar, mensurar e apoiar a mitigação de riscos cibernéticos no BCB.		
E	Aprimorar a governança do processo de compartilhamento de riscos e incidentes de segurança cibernética no âmbito do SFN.		

3. Descrição da Solução

3. Descrição da solução como um todo considerado o ciclo de vida do objeto

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste na prestação contínua, integrada e especializada de serviços de segurança cibernética, abrangendo as quatro verticais técnicas identificadas no Estudo Técnico Preliminar (ETP): gestão de vulnerabilidades, testes de invasão, inspeção de códigofonte, e modelagem de ameaças/mensuração de riscos. A solução foi definida a partir de necessidades mensuradas, riscos concretos identificados e estimativas de esforço fundamentadas em dados quantitativos relativos ao ambiente tecnológico do Banco Central do Brasil (BCB).

3.3. O ciclo de vida da solução contempla as etapas de detecção, análise, avaliação, teste, recomendação, acompanhamento e retroalimentação, de modo a assegurar continuidade e evolução da postura de segurança do BCB. Cada etapa se articula com as demais, formando um ecossistema técnico integrado e permanente ao longo da vigência contratual.

3.4. A seguir, é especificada a descrição pormenorizada de cada vertical constituinte da contratação de serviço deste projeto:

3.4.1. Gestão contínua de vulnerabilidades (tratamento de 8 vulnerabilidades diárias, 1 analista dedicado)

3.4.1.1. O serviço compreende o monitoramento, detecção, classificação e comunicação tempestiva de vulnerabilidades que afetem os mais de 9.000 ativos de TI, 6.000 softwares distintos e 1.600 projetos de códigofonte atualmente mantidos pelo BCB, em um ambiente que inclui mais de 1.200 imagens de container em produção.

3.4.1.2. Diante da projeção de crescimento global de vulnerabilidades, podendo alcançar 80.000 CVEs anuais até 2030, equivalente a aproximadamente 225 vulnerabilidades diárias, das quais entre 5 e 8 tendem a demandar tratamento específico dentro do BCB após aplicação dos fatores de atenuação, torna-se indispensável alocar um especialista dedicado exclusivamente ao processo, garantindo continuidade, tempestividade e profundidade das análises.

3.4.2. Testes de invasão contínuos (2 testes mensais, 2 analistas dedicados)

3.4.2.1. Os testes de invasão devem ocorrer de forma contínua, com capacidade mínima de 2 pentests mensais, conforme a demanda histórica e a exigência de análises antes da entrada em produção para determinados serviços.

3.4.2.2. Para atender à complexidade crescente das aplicações internas e de terceiros, bem como acompanhar o volume de sistemas em desenvolvimento, estima-se a necessidade de 160 horas de trabalho por sistema testado, em média, distribuídas entre 2 analistas especializados, garantindo profundidade, escalabilidade, cobertura adequada e resposta à variação da demanda.

3.4.3. Inspeção de código-fonte (1 teste mensal, 1 analista dedicado)

3.4.3.1. A inspeção de códigofonte deve ser executada manualmente por especialista capacitado, devido às limitações das ferramentas automatizadas (SAST) apontadas no ETP, as quais identificam apenas parcela das vulnerabilidades relevantes e não capturam falhas de lógica de negócio e fluxos complexos de dados.

3.4.3.2. Considerando que nem todas as soluções submetidas a pentest são internas, mas que o volume de sistemas próprios com criticidade e exposição relevante permanece elevado, estima-se 1 inspeção mensal, com 160 horas de trabalho por sistema, executada por 1 analista dedicado, para garantir a análise aprofundada de diferentes linguagens utilizadas no BCB (Java/Spring, .NET/C#, Node/Angular e Python).

3.4.4. Modelagem de ameaças e mensuração de riscos (8 avaliações anuais, 1 analista dedicado)

3.4.4.1. A modelagem de ameaças e a mensuração de risco devem apoiar tanto soluções internas quanto sistemas de terceiros, especialmente aqueles hospedados em ambientes de nuvem, cuja quantidade vem crescendo. A prática institucional prevê avaliações regulares, além de avaliações extraordinárias decorrentes de novos projetos e mudanças arquiteturais. Atualmente, realiza-se em média uma avaliação a cada mês e meio, com média de 240 horas por avaliação, com necessidade de 1 analista dedicado para manter regularidade, qualidade e conformidade metodológica, adotando a metodologia CISRAM v2.2.

3.4.5. Banco de horas para pentests (4000 horas, com uso máximo de 1000 horas por ano)

3.4.5.1. Considerando a volatilidade da demanda institucional e o acúmulo histórico de análises pendentes, complementa-se a solução com banco de horas específico para pentests, garantindo capacidade de absorção de picos de demanda e evitando que gargalos operacionais comprometam entregas críticas, conforme observado no ETP durante a análise comparativa de modelos de contratação.

3.5. Os serviços devem ser oferecidos integrados e articulados, com capacidade de sinergia entre serviços ao longo de todo o ciclo de vida. Os insumos produzidos em cada serviço devem ser utilizados de subsídio para as demais operações de acordo com as diretrizes a seguir:

3.5.1. Vulnerabilidades detectadas retroalimentam avaliações de risco e priorização de pentests;

3.5.2. Modelos de ameaça orientam escopos de pentest e revisão de código;

3.5.3. Resultados dos pentests subsidiam correções, aprimoramento de controles e novas avaliações.

3.5.4. Esse encadeamento contínuo foi considerado essencial para manter a maturidade e a resiliência cibernética, sendo inviável a contratação por escopos isolados, conforme análise do ETP que demonstrou perda de sinergia, retrabalho e impacto negativo na eficiência técnica caso tal modelo fosse adotado.

4. Requisitos da Contratação

Requisitos de Negócio:

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. Ter a capacidade de, com precisão, monitorar a exposição de ativos de TIC inventariados do BCB a novas vulnerabilidades descobertas;

4.1.2. Ter a capacidade de, tempestivamente, reagir à detecção de vulnerabilidades acionando um pedido de atualizações de sistemas afetados às equipes responsáveis pela manutenção de tais sistemas com orientações precisas de como solucionar o problema;

4.1.3. Ter a capacidade de, continuamente, testar a efetividade dos controles de segurança de sistemas implantados no BCB de forma escalável respondendo a variações na demanda institucional, emulando capacidades e intenções de potenciais invasores;

4.1.4. Ter a capacidade de, continuamente, testar a efetividade das funcionalidades de segurança conforme codificado nas soluções internas do BCB.

4.1.5. Ter a capacidade de, com agilidade, modelar ameaças a soluções de TIC do BCB e mensurar o risco apresentado por propostas de novas implantações de sistemas nos ambientes do BCB.

Requisitos de Capacitação

4.2. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

Requisitos Legais

4.3. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.4. Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativas e evolutivas pela natureza do objeto da contratação ser de prestação de serviço;

Requisitos Temporais

4.5. A prestação dos serviços deve ser iniciada no prazo máximo de **15** dias corridos após a assinatura do contrato, prazo esse que pode ser prorrogado, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.6. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.7. Todos os prazos citados, quando não expresso de forma diferente/específica, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.8. Na execução dos serviços, deverão ser observados os seguintes prazos:

Subitem de serviço	Atividade, Tarefa ou Serviço	Início do atendimento	Prazo máximo de conclusão
1	Notificação sobre publicação de nova vulnerabilidade relevante ao órgão	Diário	Até 1 dia útil após publicação
1	Envio de pedidos de correções de vulnerabilidades a equipe responsáveis	Semanal (Segunda a Sexta)	Sexta-feira, 16h de cada semana
1	Acompanhamento de correções	Imediato após SLA da área notificada ter vencido	Até 5 dias úteis após o vencimento do SLA
2, 4	Execução de pentest	Após reunião de apresentação	4 semanas
3	Inspeção de código fonte	Após reunião de apresentação	4 semanas
5	Modelagem de ameaças e avaliação de riscos	Após reunião de apresentação	6 semanas

4.9. Os serviços contínuos (subitens 1, 2, 3 e 5) serão prestados em dias úteis no horário de 09h00 às 12h30 e de 14h00 às 18h30.

4.10. O Banco de horas para a realização das atividades de testes de Invasão (subitem 4) seguirá as seguintes diretrizes:

4.10.1. Será realizado sob demanda e com escopo previamente definido pelo BCB.

4.10.2. O uso é limitado a 8 testes e até 1.000 horas anuais.

4.10.3. Não há garantia de consumo mínimo das horas previstas durante a vigência do contrato.

Requisitos Sociais, Ambientais e Culturais

4.11. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.11.1. A Contratada, quando cabível, deve priorizar a utilização de equipamentos e tecnologias não nocivas ao meio ambiente, com uso e aplicação de materiais e equipamentos recicláveis ou reutilizáveis.

Requisitos da Arquitetura Tecnológica

4.12. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.13. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.13.1. Todos os produtos e softwares necessários à correta prestação dos Serviços Especializados para serem instalados na infraestrutura do BCB devem estar nos padrões adotados pelo BCB.

4.13.2. Toda infraestrutura necessária para a correta execução das atividades dos serviços de forma remota, como por exemplo acesso à internet, estação de trabalho, sistema operacional etc. será de responsabilidade e deverá ser provida pela Contratada.

4.14. A solução contratada de serviço contínuo de gerenciamento de vulnerabilidades (Subitem 1) deve atender os seguintes requisitos:

4.14.1. Ser capaz de desenvolver e dar manutenção a scripts Python utilizados para acessar as APIs de sistemas de inventário e notificação de vulnerabilidades e acionar rotinas de agrupamento e priorização;

4.14.2. Ser capaz de empregar conhecimentos de análise e engenharia de dados para tratar do volume de vulnerabilidades diárias;

4.14.3. Ser capaz de gerenciar, interpretar, priorizar e compreender vulnerabilidades em sistemas hospedados, virtualizados, em containers, em Kubernetes e em projetos de código fonte.

4.14.4. Ser capaz de interagir com ferramentas de inventário de ativos e enumeração de vulnerabilidades como o Microsoft Defender, o Redhat Satelite, Redhat Insights e VMWare.

4.15. A solução contratada de serviço contínuo de inspeção de código fonte (Subitem 3) deve atender os seguintes requisitos:

4.15.1. Ser capaz de analisar as linguagens de programação Java, Python, JavaScript e C# prioritariamente.

4.15.2. Ser capaz de identificar problemas de injeções de código em interpretadores que interajam com o projeto (como SQL, Shell, etc).

4.15.3. Ser capaz de identificar vulnerabilidades de desserialização insegura.

4.15.4. Ser capaz de identificar falhas de segurança típicas em frameworks (e.g.: Spring e .NET).

4.15.5. Ser capaz de identificar uso inseguro de criptografia e APIs sensíveis.

4.16. A solução contratada de serviço contínuo de testes de invasão e banco de horas de testes de Invasão (Subitens 2 e 4) devem atender os seguintes requisitos:

4.16.1. Ter a capacidade de conduzir testes de segurança em aplicações web, incluindo aplicações de arquitetura monolítica, em 3 (três) camadas e em arquiteturas distribuídas;

4.16.2. Ter a capacidade de testar aplicações que exponham APIs REST, incluindo validação de autenticação, autorização, rate-limiting, validação de payloads, verificação de segurança de serialização/desserialização e controle de acesso baseado em contexto;

4.16.3. Ter a capacidade de testar sistemas baseados em microsserviços, avaliando a superfícies de ataque internas e externas, mecanismos de mensageria, componentes de comunicação assíncrona e serviços distribuídos;

4.16.4. Ter a capacidade de testar sistemas que façam uso de webservices SOAP, incluindo verificação de headers, esquemas XML e controles de transporte;

4.16.5. Ter a capacidade de testar aplicações construídas sobre arquiteturas baseadas em mensageria (como RabbitMQ, Kafka, ActiveMQ ou equivalentes), avaliando tópicos, filas, ACLs, mecanismos de persistência, idempotência e interceptação de mensagens;

4.16.6. Ter a capacidade de utilizar ferramentas de testes de segurança existentes no Kali Linux e o Burp Suite nos testes de segurança;

4.16.7. Ter a capacidade de priorizar, compreender e dialogar com as táticas e técnicas documentadas por frameworks de vulnerabilidades e de ataques a sistemas como o MITRE ATT&CK e o OWASP top 10.

4.17. A solução contratada de serviço contínuo de modelagem de ameaças e avaliação de riscos (subitem 5) deve atender os seguintes requisitos:

4.17.1. Empregar as metodologias de CIS RAM para o processo de avaliação de riscos;

4.17.2. Empregar o padrão e terminologia do CIS Controls para sugerir controles para as ameaças enumeradas na modelagem de ameaças;

4.17.3. Empregar técnicas de modelagem de ameaças de STRIDE, Data Flow Diagrams (DFD) e cruzamento de fronteiras de confiança.

Requisitos de Projeto e de Implementação

4.18. Não há necessidade de se exigir requisitos de projeto e de implementação, pois não está sendo contratado serviço de desenvolvimento de aplicações.

Requisitos de Implantação

4.19. Como esta contratação não implica a implantação de soluções de TIC na infraestrutura do BCB, não há requisitos de implantação previstos.

Requisitos de Garantia e Manutenção

4.20. Não se aplicam à contratação em questão.

Requisitos de Experiência Profissional e Formação da Equipe

4.21. Os requisitos de experiência profissional para a formação da equipe foram especificados nos itens que se seguem, contemplando: (a) experiência profissional, (b) formação acadêmica específica e (c) certificações de conhecimento técnico em segurança da informação.

4.21.1. As certificações de conhecimento técnico em segurança da informação especificadas nos itens que se seguem foram selecionadas a partir do painel de certificações de segurança open source de Paul Jerimy, disponível em https://pauljerimy.com /security-certification-roadmap/.

4.22. O serviço contínuo de gestão de vulnerabilidades (subitem 1) deverá ser prestado por profissionais da Contratada que atendam (satisfaçam) a pelo menos 1 (um) dos seguintes requisitos:

4.22.1. Experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em segurança cibernética, sendo pelo menos 2 (dois) anos em ações de identificar, analisar, classificar, priorizar as vulnerabilidades; propor e acompanhar mitigações.

4.22.2. Mestrado ou Doutorado com tema de pesquisa relacionado à pesquisa de vulnerabilidades, detecção de vulnerabilidades ou gestão de vulnerabilidades.

4.22.3. Uma das seguintes certificações profissionais: CISSP, GSNA, GCCC, PCI QSA, GCTI, BTL2, GEIR, eCTHP, MCPE, GCED, GSE, CISSP Concentrations, CISM, S-ISME, CCISO, EEXIN ISM, GSP, S-CISO, CASP+, CISSM, CRISC ou CGRC.

4.22.4. Duas das seguintes certificações profissionais: MDFIR, CREST CRTIA, BTL1, MBT, C)IHE, ECIR, ECIH, S-TA, CHFI, OSDA, C)TIA, GOSI, GCIA, CM) ISSO, BCS PCIRM, PEXIN ISM, MGRC, EISM, CGEIT, EXIN 27001E, PECB 27005LM, APMG 20000P, C)ISRM, APMG 27001P, PECB 27001LI, C)ISSO, C)ISSM, TUV ITSM, CIS RM, EXIN 27001P, CCRMP, PECB 27032CM, PECB 27005RM.

4.23. Os serviços relativos a testes de invasão (subitens 2 e 4) deverão ser prestados por profissionais da Contratada que atendam (satisfaçam) a pelo menos 1 (um) dos seguintes requisitos:

4.23.1. Experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em segurança cibernética, sendo pelo menos 2 (dois) anos em ações de realizar ataques cibernéticos para avaliar os controles de prevenção, detecção e resposta do órgão, além de elaborar relatórios de resultado.

4.23.2. Mestrado ou Doutorado com tema de pesquisa relacionado à descoberta de vulnerabilidades, testes de invasão ou avaliações de segurança.

4.23.3. Uma das seguintes certificações profissionais: OSCP, OSEP, OSWE, OSCE3, GXPN, GAWN, CREST CSAM, CREST CCSAS, eWPTX, MRT, PACES, CREST CCTIM, S-EHE, S-CEHL, CREST CCTINF, CREST, CRT, HTB WEE, CRTO II.

4.23.4. Duas das seguintes certificações profissionais: CRTO, GX-PT, GPEN, OSWP, LPT, PNPT, GCPN, GRTP, SOG CAPenX, GWAPT, OSMR, GCPT, MPT, CPENT, CREST CCTAPP, HTB CPTS, CSTL, eCPPT, eWPT, CMIPS, HTB CBBH, CPSH, CMWAPT, CPTC, CRTOP, CSR, eMAPT, BSCP, OPST, OSWA.

4.24. O serviço contínuo de inspeção de código fonte (subitem 3) deverá ser prestado por profissionais da Contratada que atendam (satisfaçam) a pelo menos 1 (um) dos seguintes requisitos:

4.24.1. Experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em segurança cibernética, sendo pelo menos 2 (dois) anos em (a) revisão de segurança de códigos fontes codificados prioritariamente na linguagem Java e secundariamente em Python, Javascript e C#, e em (b) descoberta de vulnerabilidades contemplando a identificação de (b.1) problemas comuns de regras de negócio e (b.2) trajetórias inseguras de dados, por meio de análise source-sink ou com AppSec ou Code Review manual.

4.24.2. Mestrado ou Doutorado com tema de pesquisa relaciona à programação segura, descoberta de vulnerabilidades, engenharia de exploits, engenharia reversa ou DevSecOps.

4.24.3. Uma das seguintes certificações profissionais: GWEB, OSCP, OSEP, OSWE, OSCE3, GXPN, GAWN, CREST CSAM, CREST CCSAS, eWPTX, MRT, PACES, CREST CCTIM, S-EHE, S-CEHL, CREST CCTINF, CREST, CRT, HTB WEE, CRTO I.

4.24.4. Duas das seguintes certificações profissionais: S-CSPL, CSSLP, DevNet Pro, CASE (das linguagens Java, Python ou C#), GMLE, CASST, DevNet A, CRTO, GX-PT, GPEN, OSWP, LPT, PNPT, GCPN, GRTP, SOG CAPenX, GWAPT, OSMR, GCPT, MPT, CPENT, CREST CCTAPP, HTB CPTS, CSTL, eCPPT, eWPT, CMIPS, HTB CBBH, CPSH, CMWAPT, CPTC, CRTOP, CSR, eMAPT, BSCP, OPST, OSWA.

4.25. O serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (subitem 5) deverá ser prestado por profissionais da Contratada que atendam (satisfaçam) a pelo menos 1 (um) dos seguintes requisitos:

4.25.1. Experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em segurança cibernética, sendo pelo menos 2 (dois) anos em modelagem de ameaças, avaliações de risco ou arquitetura segura.

4.25.2. Mestrado ou Doutorado com tema de pesquisa relacionado à modelagem de ameaças ou avaliação de riscos.

4.25.3. Uma das seguintes certificações profissionais: GSE, CISSP Concentrations, CISM, S-ISME, CISSP, CCISO, EEXIN ISM, GSP, S-CISO, CASP+, CISSM, CRISC ou CGRC.

4.25.4. Duas das seguintes certificações profissionais: CM)ISSO, BCS PCIRM, PEXIN ISM, MGRC, EISM, CGEIT, EXIN 27001E, PECB 27005LM, APMG 20000P, C)ISRM, APMG 27001P, PECB 27001LI, C)ISSO, C)ISSM, TUV ITSM, CIS RM, EXIN 27001P, CCRMP, PECB 27032CM, PECB 27005RM.

Requisitos de Metodologia de Trabalho

4.26. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

4.27. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.28. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento **8** horas por dia e **5** dias por semana de maneira eletrônica e **8** horas por dia e **5** dias por semana por via telefônica.

4.29. A execução do serviço dever ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.30. A fiscalização da execução do contrato avaliará o resultado dos serviços pelos artefatos entregáveis produto dos serviços como relatórios de testes, mensagens de pedidos de correção de vulnerabilidades e modelos de ameaças.

Requisitos de Segurança da Informação e Privacidade

4.31. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos na Política de Segurança da Informação (PSIBC) da Contratante.

4.32. A CONTRATADA deverá possuir, durante toda a vigência contratual, licenciamento válido de ferramenta profissional de análise de segurança em abordagem caixa-preta, destinada à identificação automatizada e assistida de vulnerabilidades em aplicações, serviços, APIs e ativos expostos, contemplando recursos de inteligência artificial para apoio à detecção, priorização, correlação ou interpretação de achados para os profissionais alocados para prestar os serviços previstos nos subitens 2 e 4 da tabela 1.2, então contemplando a disponibilidade pelo menos 3 licenças.

4.32.1. A ferramenta deverá:

I. Ser licenciada para uso corporativo e comercial;

II. Permitir a realização de análises automatizadas e assistidas, contribuindo para a padronização metodológica e para a redução da variabilidade entre análises realizadas por diferentes profissionais;

III. Disponibilizar mecanismos de apoio baseados em inteligência artificial para aprimoramento da eficiência operacional e aumento da cobertura das análises;

IV. Possuir documentação pública do fabricante quanto às políticas de tratamento de dados e às garantias de privacidade aplicáveis aos recursos de inteligência artificial;

V. Garantir contratualmente, por meio dos termos de licenciamento, política do fabricante ou compromisso formal equivalente, que os dados processados pela solução, incluindo conteúdos submetidos por usuários, resultados de varreduras, artefatos coletados, códigos, configurações, evidências e demais informações decorrentes da execução dos serviços:

a) não sejam utilizados para treinamento, retreinamento ou aprimoramento de modelos fundacionais ou de inteligência artificial destinados a terceiros;

b) não sejam compartilhados com outros clientes ou ambientes externos à prestação do serviço;

c) sejam tratados de acordo com controles de segurança compatíveis com a criticidade das informações processadas.

VI. Permitir a emissão de evidências e registros que suportem tecnicamente as conclusões apresentadas nos relatórios entregues à CONTRATANTE.

4.32.2. A exigência de ferramenta profissional de análise de segurança com recursos de inteligência artificial visa assegurar níveis mínimos de qualidade, consistência, rastreabilidade e eficiência na execução dos serviços especializados de segurança cibernética.

4.32.3. A utilização de plataforma profissional amplamente consolidada no mercado reduz a dependência exclusiva da análise manual dos profissionais alocados, permitindo maior uniformidade metodológica, ampliação da cobertura dos testes, redução da probabilidade de omissão de vulnerabilidades e aumento da produtividade na identificação, correlação e priorização de riscos.

4.32.4. Adicionalmente, considerando que soluções modernas de segurança incorporam funcionalidades baseadas em inteligência artificial, mostra-se necessário estabelecer requisitos mínimos de governança e proteção de dados. Tais requisitos visam mitigar riscos relacionados ao tratamento de informações potencialmente sensíveis da infraestrutura da CONTRATANTE, garantindo que dados submetidos à ferramenta não sejam utilizados para treinamento ou aprimoramento de modelos de inteligência artificial acessíveis a terceiros, evitando eventual exposição indevida de informações estratégicas ou de segurança.

4.32.5. A exigência não se destina à restrição da competitividade ou à seleção de fabricante específico, mas à demonstração de capacidade operacional mínima compatível com a complexidade dos serviços contratados e com os requisitos de segurança da informação exigidos pela Administração.

4.32.6. Constitui responsabilidade exclusiva da CONTRATADA prover e manter, durante toda a execução contratual, as licenças de software, assinaturas corporativas, recursos de inteligência artificial, créditos de utilização, tokens de processamento, capacidade computacional e quaisquer outros recursos tecnológicos necessários ao cumprimento das atividades previstas neste Termo de Referência.

4.32.7. Eventual insuficiência de créditos, tokens, capacidade de processamento ou limitações decorrentes do licenciamento das soluções adotadas pela CONTRATADA não constituirá justificativa para atraso, indisponibilidade, redução de escopo, degradação da qualidade dos serviços ou solicitação de reequilíbrio econômico-financeiro do contrato.

Vistoria

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

Sustentabilidade

4.34. Não se aplica nesta contratação critérios e práticas de sustentabilidade, por se tratar de aquisição de serviços, sem bens físicos (licença de software e prestação de serviços continuados de segurança da informação).

Indicação de marcas ou modelos

4.35. Pela natureza do objeto da contratação, não há indicação de marcas ou modelos para esta contratação.

Da vedação de utilização de marca/produto na execução do serviço

4.36. Pela natureza do objeto da contratação, não há vedação de marcas ou modelos para esta contratação.

Da exigência de carta de solidariedade

4.37. Não será exigida carta de solidariedade pela natureza do objeto da contratação.

Subcontratação

4.38. Não será admitida a subcontratação do objeto contratual.

Garantia da contratação

4.39. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021.

4.39.1. A justificativa para a não exigência de garantia é o fato da contratação não prever pagamentos antecipados nem desembolso de recursos sem a correspondente comprovação da execução dos serviços, reduzindo significativamente o risco de prejuízo financeiro direto à Administração em caso de inadimplemento.

4.39.2. A execução contratual será acompanhada por fiscalização contínua, com pagamentos condicionados à efetIva prestação dos serviços e ao aceite das entregas, o que reduz a exposição da Administração ao risco de inadimplemento contratual.

4.39.3. O instrumento contratual prevê mecanismos de mitigação de riscos, incluindo multas moratórias e compensatórias, possibilidade de retenção de pagamentos, glosas, além das demais sanções previstas na Lei nº 14.133/2021, de forma que a garantia contratual não se mostra imprescindível para a proteção do interesse público.

Margem de Preferência

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

Informações relevantes para o dimensionamento e apresentação da proposta

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

4.41.1. Para o serviço contínuo de gestão de vulnerabilidades (Subitem 1), é estimado um esforço de tratamento de 8 (oito) vulnerabilidades diárias, indicando uma quantidade recomendada de 1 (um) analista dedicado;

4.41.2. Para o serviço contínuo de testes de invasão (pentesting) (Subitem 2), é estimado um esforço de realização de 2 (dois) testes de invasão por mês, indicando uma quantidade recomendada de 2 (dois) analistas dedicados;

4.41.3. Para o serviço contínuo de inspeção de segurança de código fonte (Subitem 3), é estimado um esforço de 1 (uma) inspeção de código fonte por mês, indicando uma quantidade recomendada de 1 (um) analista dedicado;

4.41.4. Para o serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (Subitem 5), é estimado um esforço de 8 avaliações anuais, indicando uma quantidade recomendada de 1 analista dedicado;

4.41.5. Para o uso de banco de horas de teste de invasão (Subitem 4), o fornecedor deve dimensionar sua equipe para ser capaz de executar até 1.000 horas de pentest sob demanda por ano.

5. Papéis e Responsabilidades

5.1. São obrigações da CONTRATANTE:

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

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

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

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis.

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

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

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

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

5.2. São obrigações do CONTRATADO:

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

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

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

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

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

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

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

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

5.2.9. responsabilizar-se pela gestão administrativa dos profissionais da equipe de prestação de serviços; não haverá relação de subordinação hierárquica entre os profissionais e os servidores do BCB;

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

5.2.11. apresentar formulário de identificação e dados pessoais/sociais, preenchido e assinado individualmente por todos os profissionais alocados para a prestação dos serviços, incluindo substitutos e preposto, nos moldes previstos pelo Departamento de Segurança do Banco Central do Brasil, antes do início da vigência do contrato e sempre que houver apresentação de novos funcionários, ou ainda mediante solicitação do BCB. O referido formulário não configura requisito para habilitação de empresas e não isenta a CONTRATADA da responsabilidade pela escolha e seleção de empregados idôneos, respeitando as diretrizes contratuais estabelecidas pelo CONTRATANTE;

6. Modelo de Execução do Objeto

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: no prazo máximo de 15 (quinze) dias corridos após a assinatura do contrato, prazo esse que pode ser prorrogado, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante.

6.1.2. A contratada, no momento da assinatura do contrato, deverá fornecer o nome, telefone e endereço corporativo de correio eletrônico dos detentores dos cargos listados a seguir e mantê-los atualizados no decorrer do contrato, os quais poderão ser acionados no caso de persistência de eventuais contendas:

Tabela de Escalonamento

Nível	BCB	Contratada
1	Chefe Adjunto de Departamento	Diretor de Vendas e/ou Diretor de operações
2	Chefe de Subunidade e/ou fiscal administrativo do contrato	Gerente de Vendas Nacional
3	Coordenador e/ou fiscal técnico do contrato	Gerente de Conta
4	Fiscal requisitante do contrato	Preposto

6.1.3. Uma reunião inicial será realizada com a Contratada em até 15 (quinze) dias corridos após a assinatura do contrato, que será feita por meio de conferência virtual.

6.1.4 Caberá à CONTRATADA a gestão administrativa dos prestadores de serviço do contrato, de modo que não haverá relação de subordinação hierárquica entre os profissionais e os servidores do BCB.
6.1.5 No modelo de execução dos serviços, a comunicação ocorrida entre os profissionais da CONTRATADA e as demais partes atuantes da equipe de segurança de TIC não configuram transmissão de ordens entre as partes, mas sim simples intercâmbio de informações, necessário para a plena execução dos serviços e para a adequada gestão e acompanhamento técnico dos serviços prestados.

Local e horário da prestação dos serviços

6.2. Os serviços serão prestados na modalidade remota, não sendo necessária a prestação de serviço in loco na sede do BCB em Brasília;

6.3. Os serviços serão prestados em dias úteis no horário das 9h00 às 12h30 e das 14h00 às 18h30, horário de Brasília, conforme dias de funcionamento da Sede do BCB em Brasília.

Rotinas a serem cumpridas

6.4. A execução contratual observará as rotinas definidas para cada serviço contínuo detalhado a seguir:

6.5. Rotinas para o serviço contínuo de gestão de vulnerabilidades (subitem 1)

6.5.1. Rotina de monitoramento de novas vulnerabilidades: Acompanhar diariamente a publicação de novas vulnerabilidades que afetem ativos de interesse do órgão. Pode ser informado via portais de notícias, de publicação de Threat Intelligence ou utilizando os canais de automação de coleta do órgão como o Defender, Redhat Insights, ou solução própria baseada em python, então tendo a capacidade de contribuir com melhorias para esta automação para aumentar a sua efetividade.

6.5.2. Rotina de priorização de vulnerabilidades: Realizar uma seleção de vulnerabilidades que apresentam o maior risco ao órgão, agregando informações para priorização como facilidade de exploração, existência de agentes a explorando sendo noticiados e impacto.

6.5.3. Rotina de notificação para atualização de ativos: Notificar equipes responsáveis pelos ativos afetados pelas vulnerabilidades, interagindo, esclarecendo e os orientando quanto à importância da correção e sobre como corrigir a vulnerabilidade.

6.5.4. Rotina de acompanhamento da efetividade das atualizações: Monitorar a efetividade de notificações já realizadas acompanhando o número de ativos ainda expostos às vulnerabilidades notificadas. Em caso de não correção em tempo hábil, manter diálogo com a equipe notificada para obter esclarecimentos de motivos para a não correção.

6.6. Rotinas para o serviço contínuo de testes de invasão (subitem 2)

6.6.1. Rotina de coleta de informação: Esta rotina caracteriza o início do processo. Envolve o recebimento de documentação técnica disponível sobre a solução a ser avaliada e uma reunião inicial de apresentação da solução. Tem como produto um plano de testes baseado em hipóteses.

6.6.2. Rotina de execução do teste de invasão: Executar os testes enumerados no plano de testes registrando achados e o expandindo conforme descobre mais informações.

6.6.3. Rotina de elaboração de relatório: Sintetizar o resultado do teste em um relatório a ser informado à área demandante do teste de vulnerabilidade. Nele, apontar a causa raiz das fragilidades encontradas, sugerindo controles de mitigação.

6.6.4. Rotina de aprimoramento de scripts de priorização e automação de tratamento de vulnerabilidades: O processo de triagem de vulnerabilidades é assistido por scripts de automação de priorizações e cruzamento de informações ativos. Na medida da necessidade e oportunidade, dar manutenção e incrementar melhorias para tais scripts do BCB.

6.7. Rotinas para o serviço contínuo de inspeção de código fonte (subitem 3)

6.7.1. Rotina de coleta de informação: Esta rotina caracteriza o início do processo. Envolve o recebimento de documentação técnica disponível sobre a solução a ser avaliada, acesso ao código fonte e uma reunião inicial de apresentação da solução.

6.7.2. Rotina de inspeção do código fonte: Passa por compreender o sistema, produzindo um modelo de ameaças para identificar os ativos em risco e meios de vulnerá-los. Também coleta informações a viabilidade de comprometer determinadas fontes de informações.

6.7.3. Rotina de elaboração de relatório: Sintetizar o resultado da inspeção em um relatório a ser informado à área demandante da análise. Nele, apontar a causa raiz das fragilidades encontradas, sugerindo controles de mitigação.

6.7.4. Rotina de contextualização de CVEs em dependências de projetos: É uma rotina de apoio ao serviço contínuo de gestão de vulnerabilidades. Consiste em agrupar e priorizar vulnerabilidades relativas a bibliotecas, pacotes ou dependências que constituam a Software Bill of Material (SBOM) de projetos mantidos internamente pelo órgão, cabendo orientar o profissional responsável por esta gestão de vulnerabilidades sobre como ser o melhor método de correção da vulnerabilidade, que equipes de desenvolvimento notificar e como comunicar o pedido de correção.

6.7.5. Rotina de detecção de ameaças no ambiente relativas a comprometimento de cadeia de suprimentos (Supply Chain): É uma rotina de apoio ao serviço contínuo de gestão de vulnerabilidades. Consiste em investigar nos repositórios de dependências do órgão pela presença de pacotes anunciados como vulneráveis ou maliciosos para complementar o diagnóstico e detecção de exposição realizado.

6.7.6. Rotina de consultoria de análise de resultados de ferramentas automatizadas de análise estática de código: O prestador de serviço fica disponível e acessível pelos canais de comunicação acordados para ser consultado para esclarecer dúvidas enviadas por desenvolvedores do órgão relativas a resultados de analisadores automáticos de código eventualmente empregados em esteira de automação de integração contínua de código.

6.8. Rotinas para o serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (subitem 5)

6.8.1. Rotina de coleta de informação: Esta rotina caracteriza o início do processo. Envolve o recebimento de documentação técnica disponível sobre a solução a ser avaliada e uma reunião inicial de apresentação da solução.

6.8.2. Rotina de modelagem de ameaças: Com as informações coletadas, elabora um modelo sobre a solução que sintetiza as suas informações relevantes para o escopo de uma análise de segurança. Este modelo deve descrever sucintamente o seu funcionamento básico, ativos que a solução depende, manipula, interage e acessa que poderiam ser afetados em seu eventual comprometimento e níveis de exposição (operadores administradores, rede interna, exposto na internet). Então agregar a este modelo descritivo inferências de possíveis ameaças que podem afetar o órgão a partir dos componentes descritos da solução. Finalmente, enumerar possíveis controles intrínsecos (e.g.: Políticas de segurança a serem habilitados em painel de configurações da solução) e controles extrínsecos (e.g.: Segregar a solução em uma rede isolada).

6.8.3. Rotina de mensuração: Realizada coletivamente com os demais colaboradores da área de segurança cibernética, apresenta o modelo elaborado e discute as probabilidades das ameaças enumeradas, balizada pelos controles já implementados, e discutindo a pertinência de cada controle sugerido.

6.8.4. Rotina de elaboração de relatório: Sintetizar o resultado do cálculo de risco em um relatório a ser informado à área demandante da avaliação de risco. Nele, apontar as ameaças que apresentarem risco indesejável para os parâmetros do órgão, sugerindo os controles discutidos na rotina de mensuração.

6.8.5. Rotina de complementação de documentação de segurança de projetos: É uma rotina de apoio aos serviços contínuos de testes de invasão e inspeção de código fonte. Consiste em colaborar com estes serviços com a formulação de diagramas de modelos de ameaças e sugestão de hipóteses e apoio à elaboração do plano de teste. A documentação resultante desta rotina seria anexada à documentação da equipe de desenvolvimento da solução.

Materiais a serem disponibilizados

6.9. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários.

Informações relevantes para o dimensionamento da proposta

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

6.10.1. Serviço contínuo de gestão de vulnerabilidades (subitem 1);

6.10.1.1. O esforço estimado para o serviço é de tratamento de 8 vulnerabilidades diárias. Admitindo que o tratamento de uma vulnerabilidade exija um esforço de 1 (uma) hora, recomenda-se a prestação por 1 (um) profissional;

6.10.2. Serviço contínuo de testes de invasão (subitem 2);

6.10.2.1. O esforço estimado para o serviço é de 2 (dois) testes mensais, sendo recomendada a prestação por 2 (dois) profissionais;

6.10.3. Serviço contínuo de inspeção de código fonte (subitem 3)

6.10.3.1. O esforço estimado para o serviço é de 1 (uma) avaliação mensal, sendo recomendada a prestação por 1 (um) profissional;

6.10.4. Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (subitem 5)

6.10.4.1. O esforço estimado para o serviço é de 8 (oito) avaliações anuais, sendo recomendada a prestação por 1 (um) profissional;

Formas de transferência de conhecimento

6.11. Eventuais scripts, programas, planilhas e outros artefatos desenvolvidos para apoio aos serviços contínuos devem ter seu conhecimento transferido aos servidores do BC.

Procedimentos de transição e finalização do contrato

6.12. Eventuais scripts, programas, planilhas e outros artefatos desenvolvidos para apoio aos serviços contínuos devem ter seu conhecimento transferido aos servidores do BC, possibilitando sua transição para um novo contrato.

Quantidade mínima de serviços para comparação e controle

6.13. Não será necessário a entrega de bens ou serviços para comparação e controle.

Mecanismos formais de comunicação

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

I. Ordem de Serviço;
II. Ata de Reunião;
III. Ofício;
IV. Sistema de abertura de chamados;
V. E-mails e Cartas;

6.15. Os mecanismos preferíveis para comunicação são o E-mail e telefone, com as seguintes diretrizes:

6.15.1. Para as atividades de varredura pontuais, inspeções de código fonte e testes de invasão (serviço contínuo), incluídas nos subitens 1, 2 e 3, será utilizado sistema de abertura de chamados com registro rastreável fornecido pelo BCB, quando couber.

6.15.2. Para uso do Banco de horas do subitem 4, o BCB acionará a Contratada pelo número de telefone fornecido ou e-mail e explicará a esta as atividades que precisarão ser realizadas, com o escopo a ser definido em reunião específica com a Contratada.

6.15.3. Será adotado o uso de ofícios quando a resposta a e-mails enviados não for satisfatória e, também, para a notificação de não conformidades que possam vir a dar causa a aplicação de sanções.

Manutenção de Sigilo e Normas de Segurança

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

6.17. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, encontra-se no ANEXO 2.

6.18. O Modelo de Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se no ANEXO 3.

7. Modelo de Gestão do Contrato

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

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

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

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

7.6. O Contratado não necessitará manter preposto da empresa no local da execução do objeto durante o período de vigência do contrato.

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

Reunião Inicial

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

7.9. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 15 (quinze) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.10. A pauta desta reunião observará, pelo menos:

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

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

7.10.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

Rotinas de Fiscalização

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

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.14. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.15. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

7.18. A fiscalização da execução dos serviços contratados avaliará as entregas segundo os seguintes critérios:

7.18.1. Suficiência: critério de avaliação sobre o serviço verificando o cumprimento de todas as etapas e rotinas esperadas para o tempo e contexto acordados. É avaliado por instrumentos de acompanhamento como Checklists ou Planilhas de Acompanhamento de Processos. A falta de execução de alguma etapa ou rotina deverá ser formalmente justificada, sendo passível de sanção caso a justificativa seja inexistente ou inadequada. Admite-se renegociação de etapas e rotinas esperadas com o fiscal requisitante ou o fiscal técnico do contrato com a adição ou remoção de etapas com o objetivo de aprimorar a prestação do serviço ao longo da vigência do contrato.

7.18.2. Qualidade: critério de avaliação sobre o serviço verificando os produtos intermediários e finais elaborados pela prestação do serviço como relatórios e documentos. É avaliado pela correspondência destes produtos à capacidade de responder às perguntas que se espera de serem respondidas pelo instrumento. As perguntas específicas são definidas detalhadamente para cada caso de serviço especificado. O fiscal ainda pode solicitar complementações ao resultado do serviço sem custo adicional, caso o produto esteja incompleto.

7.18.3. Tempestividade: critério de avaliação sobre o serviço verificando a celeridade com a qual as etapas e rotinas previstas são realizadas. É avaliado pelo intervalo de tempo entre os marcos temporais de rotinas de serviço devidamente registrados em e-

mails e na plataforma de gerenciamento de serviços do órgão. Atrasos eventuais devem ser devidamente justificados, sendo passível de sanção e glosa caso a justificativa seja inexistente ou inadequada. Admite-se uma tolerância de 5 dias de atraso em relação aos prazos estipulados, exceto para o serviço de subitem 1 da tabela 1.2, que opera com prazos de tratamento menores.

7.18.4. Clareza: critério de avaliação sobre o serviço verificando a legibilidade na comunicação dos resultados. Os registros escritos em canais de comunicação utilizados para conduzir as rotinas de serviço são avaliados por sua precisão e concisão técnica, e não reincidência em fornecimento de informações ambíguas, vagas, incompletas, incorretas ou contraditórias que resultem em disrupção operacional das atividades cotidianas do órgão.

7.18.5. Relevância: critério de avaliação sobre o serviço verificando a devida pertinência e priorização dos escopos e enfoques adotados para a execução das rotinas definidas. É avaliado pela comparação de métricas acordadas como referenciais de priorização previamente acordados dos objetos tomados como escopo ou enfoque contra as demais opções de objetos disponíveis no momento da avaliação. A prioridade pode ser redefinida durante a vigência do contrato a qualquer tempo por demanda institucional. Resultados que não respeitaram a priorização definida devem ser devidamente justificados, sendo passível de sanção caso a justificativa seja inexistente ou inadequada.

7.18.6. A tabela a seguir sintetiza os instrumentos utilizados para medir a glosa a ser aplicada nas parcelas de pagamentos para cada critério definido de fiscalização:

Critérios	Instrumento de medição para glosa
Suficiência	Itens previstos não cumpridos em relação ao total.
Qualidade	Perguntas esperadas dos produtos dos serviços não respondidas em relação ao total.
Tempestividade	Dias de atraso divididos pelo prazo de tolerância de 5 dias, excetuando-se para o subitem 1 da tabela 1.2.
Clareza	Número de retrabalhos de ato de comunicação que tenha resultado em disrupção de operações do órgão.
Relevância	Características não utilizadas para priorização em relação ao total.

7.19. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

7.19.1. A fiscalização técnica do serviço contínuo de gestão de vulnerabilidades (subitem 1 da tabela 1.2), avaliará os critérios de fiscalização da seguinte forma:

7.19.1.1. Suficiência: Pelo menos 5 (cinco) notificações de correção de vulnerabilidades são emitidas relacionadas a vulnerabilidades e ativos distintos por semana (ajustável dependendo da semana tiver feriado prolongado). Para toda notificação emitida, acompanhar a evolução de sua correção entrando em contato com a área responsável caso ao término do prazo de acordo de nível de serviço para a correção da vulnerabilidade a exposição dos ativos afetados não mudar significativamente. Notificações repetidas sobre o mesmo ativo e vulnerabilidade não configuram notificações distintas.

7.19.1.2. Qualidade: Dois produtos são avaliados: mensagens de notificação para correção de vulnerabilidades e relatório de acompanhamento de correções. A prestação do serviço será considerada de qualidade caso respondam às seguintes perguntas:

7.19.1.2.1. Quais ativos estão vulneráveis?

7.19.1.2.2. Quais vulnerabilidades estão afetando os ativos?

7.19.1.2.3. O que a vulnerabilidade mais crítica do conjunto pode impactar o ativo e o órgão se explorado?

7.19.1.2.4. Quais são os agravantes de urgência desta vulnerabilidade? (contemplando grau de exposição à internet do ativo afetado, existência noticiada de agentes de ameaça explorando a vulnerabilidade, ou facilidade de exploração da vulnerabilidade)

7.19.1.2.5. Como a vulnerabilidade é corrigida?

7.19.1.2.6. Como a vulnerabilidade é explorada? (Sem a necessidade de detalhar tecnicamente a vulnerabilidade, mas enumerar os meios de acionamento da vulnerabilidade para que a equipe responsável possa tomar medidas paliativas enquanto não existe correção definitiva disponível).

7.19.1.2.7. Desde a última notificação relacionada a correções de vulnerabilidades em um produto até o prazo acordado de correção, houve queda significativa de ativos expostos?

7.19.1.3. Tempestividade: Os critérios de tempestividade que serão avaliados coincidem com os prazos definidos nas seções de Requisitos Temporais (item 4.8), repetidos a seguir:

7.19.1.3.1. Na execução dos serviços, deverão ser observados os seguintes prazos:

Subitem de Serviço da tabela do item 1.2	Atividade, Tarefa ou Serviço	Início do atendimento	Prazo máximo de conclusão
1	Notificação sobre publicação de nova vulnerabilidade relevante ao órgão	Diário	Até 1 dia útil após publicação
1	Envio de pedidos de correções de vulnerabilidades a equipe responsáveis	Semanal (Segunda a Sexta)	Sexta-feira, 16h de cada semana
1	Acompanhamento de correções	Imediato após SLA da área notificada ter vencido	Até 5 dias úteis após o vencimento do SLA
2, 4	Execução de pentest	Após reunião de apresentação	4 semanas
3	Inspeção de código fonte	Após reunião de apresentação	4 semanas
5	Modelagem de ameaças e avaliação de riscos	Após reunião de apresentação	6 semanas

7.19.1.4. Clareza: as notificações de correções de vulnerabilidades emitidas às equipes de manutenção e desenvolvimento responsáveis por corrigir as vulnerabilidades serão reconhecidas como claras caso tais equipes apliquem as correções necessárias para mitigar a vulnerabilidade e atendam a solicitação no prazo adequado à urgência declarada na mensagem. A contratada não será penalizada em casos em que o pedido é evidentemente claro, mas não implicou em ações adequadas das áreas responsáveis por razões que extrapolam as limitações da comunicação. A contratada deve corrigir imediatamente inconsistências apontadas pelo fiscal.
7.19.1.5. Relevância: as notificações de correções de vulnerabilidades realizadas durante cada semana serão reconhecidas como relevantes caso utilize as seguintes características para priorização:
7.19.1.5.1. Métricas de pontuação de severidade de vulnerabilidade atribuídos por organizações terceiras reconhecidas como o EPSS ou o CVSS. Deverão ser priorizadas as vulnerabilidades de severidade críticas, seguidas das altas, seguidas médias e seguidas das baixas.
7.19.1.5.2. Informações agregadas que contextualize a facilidade de exploração da vulnerabilidade como se há ferramenta de exploração pública disponível.
7.19.1.5.3. Informações agregadas que contextualize a urgência de correção como se há agentes de ameaças a explorando sendo noticiados. Em caso de vulnerabilidade em que não há remediação disponível (zero-day), a contratada deverá sugerir um conjunto de controles paliativos para mitigar a ameaça.
7.19.1.5.4. Informações agregadas sobre se estão afetando ativos com maior exposição na internet.
7.19.1.5.5. Vulnerabilidades publicadas de softwares de fabricantes indicadas pelo BC como relevantes devem ser priorizadas excepcionalmente.
7.19.2. A fiscalização técnica do serviço contínuo de testes de invasão (subitem 2 da tabela 1.2) e do uso do banco de horas de testes de invasão (subitem 4 da tabela 1.2), avaliará os critérios de fiscalização da seguinte forma:

7.19.2.1. Suficiência: A suficiência do serviço será avaliada pelo conteúdo do relatório de teste. Será avaliado se o escopo delimitado é pertinente com o prazo acordado. As evidências de suficiência utilizadas serão a correspondência de seções e conteúdo no relatório de teste com as seções sugeridas pelas metodologias de teste de invasão públicas (e.g.: OWASP, PTES, NIST 800-115, OSSTMM, etc) e o registro de evidências obtidas durante os testes anexados ao relatório como prints e logs, sendo possível recorrer a hashes de artefatos ou prints parcialmente censurados como evidência quando se tratar de conteúdo sensível ou crítico. Será considerado uma entrega insuficiente quando se verificar: ausência de tentativas de exploração quando houver indícios; não testagem de superfície crítica; ou aplicação de metodologia incompatível com o escopo. Para o escopo, será verificado se:

7.19.2.1.1. O escopo contempla todos os ativos críticos e todas as superfícies de ataque e acesso que alcancem direta ou indiretamente tais ativos críticos.

7.19.2.1.2. A extensão da agenda de testes e hipóteses cobre um escopo razoável de dúvidas sobre a segurança do escopo avaliado.

7.19.2.1.3. A profundidade com a qual cada hipótese e teste é investigado é capaz de falsear ou comprovar a hipótese proposta.

7.19.2.1.4. O Relatório contém seção de Relatório executivo, contendo resumo gerencial e estratégico das ações realizadas, das vulnerabilidades encontradas e das falhas exploradas;

7.19.2.1.5. O Relatório contém seção de Relatório técnico, que detalha em nível técnico as ações realizadas, as vulnerabilidades encontradas e as falhas exploradas.

7.19.2.2. Qualidade: A prestação do serviço será considerada de qualidade caso o relatório de teste responda às seguintes perguntas:

7.19.2.2.1. Quais os achados para a agenda de testes elaborada?

7.19.2.2.2. Como os achados foram identificados (com detalhes sobre ferramentas utilizados e sequência de investigação)?

7.19.2.2.3. Quais ativos foram afetados?

7.19.2.2.4. Como reproduzir o achado e quais são as condições necessárias para a sua exploração (com fornecimento de script ou prova de conceito verificável, quando aplicável)?

7.19.2.2.5. Qual o impacto realista se explorado?

7.19.2.2.6. Quais são as soluções sugeridas graduadas em termos de facilidade de instalação, custos, urgência e efetividade do controle (diferenciando controles paliativos dos definitivos)?

7.19.2.3. Tempestividade: Como instrumento de medição serão utilizadas as datas e horários imputados em eventos de baixa e entrega no sistema interno de gerenciamento de serviços do órgão. O prazo só começará a correr após a entrega do escopo final, concessão integral dos acessos necessários para o teste, e fornecimento de janela autorizada de execução do teste. O prazo não começará a correr para chamados abertos que excedam a capacidade de atendimento contratada de 2 (duas) avaliações mensais. Eventuais indisponibilidades ou atrasos por fatores imputáveis à Contratante suspendem a contagem do prazo. Na hipótese de achados críticos, conforme pedido da Contratante, emitir uma notificação imediata para os responsáveis pelo sistema avaliado imediatamente, independentemente do prazo do relatório. O serviço será avaliado em termos de tempestividade ao finalizar a entrega do relatório de teste conforme o prazo padrão de 4 semanas.

7.19.2.4. Clareza: O serviço será avaliado em termos de clareza pelo relatório de análise elaborado ao final de cada teste de invasão. A comunicação dos achados deve ser objetiva, sem ambiguidades que possam requerer retrabalho. Como instrumento de medição e potencial condição para a glosa será utilizado o número de retrabalhos necessários por conta de resultados insuficientemente documentados e que necessitem de mais esclarecimentos.

7.19.2.5. Relevância: A relevância será apurada a partir da leitura do relatório de análise. O serviço será avaliado em termos de relevância ao verificar que as superfícies de ataque, hipóteses de vulnerabilidade e ativos priorizados no escopo de teste acumulam características de agravantes de risco como:

7.19.2.5.1. Estar relacionado a um ativo ou processo crítico;

7.19.2.5.2. Grau de exposição a redes externas;

7.19.2.5.3. Emprego de técnicas e táticas em evidência coletadas das fontes do órgão de inteligência de ameaças.

7.19.3. A fiscalização técnica do serviço contínuo de inspeção de código fonte (subitem 3 da tabela 1.2), avaliará os critérios de fiscalização com base no relatório resultante de análise da seguinte forma:

7.19.3.1. Suficiência: Será verificado se todo o escopo de análise está contemplado no relatório de análise. A suficiência não será avaliada como mera cobertura de todo o código fonte, mas apenas as superfícies de ataque relevantes de serem analisadas como interfaces, pontos de acesso de usuários, fluxos críticos e a sequência relacionada com análises de fonte-foz (source-sink). O instrumento de medição utilizado será checklist e planilhas de acompanhamento validando se todas as hipóteses enumeradas nesta seção foram cobertas e validação de correspondência de investigações sugeridas por manuais de metodologias públicas de inspeção contra o relatório resultante de análise (e.g.: OWASP Code Review Guide; CERT Secure Coding Standards; NIST SSDF). Nas análises, espera-se validar se o código está resistente, pelo menos, às seguintes fragilidades:

7.19.3.1.1. Injeções de código, seja shell, SQL ou por outro interpretador com o qual interaja;

7.19.3.1.2. Reflexividade e Desserializações inseguras;

7.19.3.1.3. Descompactações inseguras (e.g.: Zip Bomb e Zip Slip) e aceitação de arquivos com path traversal.

7.19.3.1.4. Validar se o código está com regras de negócio bem definidas resistente à exploração de erros lógicos;

7.19.3.1.5. Validar se o código está com regras de negócio bem definidas resistente à sequestro de sessões autenticadas;

7.19.3.1.6. Validar se o código está com regras de negócio bem definidas resistente à uso inseguro de criptografia;

7.19.3.1.7. Validar se o código está com regras de negócio bem definidas resistente a seções de autenticação e autorização inadequadas.

7.19.3.2. Qualidade: A prestação do serviço será considerada de qualidade caso o relatório responda de forma objetiva às seguintes perguntas:

7.19.3.2.1. Quais vulnerabilidades foram identificadas no código?

7.19.3.2.2. Em que arquivo, linha ou função ocorre o problema?

7.19.3.2.3. Como reproduzir ou verificar a falha manualmente com o sistema em funcionamento?7.19.3.2.4. Qual a causa raiz do problema no código?

7.19.3.2.5. Qual o impacto realista caso explorado?

7.19.3.2.6. Quais são as recomendações de correção, graduadas por clareza da solução, esforço de desenvolvimento, custo e tempo, urgência e efetividade dos controles (diferenciando controles paliativos dos definitivos)?

7.19.3.3. Tempestividade: Como instrumentos de medição serão utilizadas as datas e horários imputados em eventos de baixa e entrega no sistema interno do órgão de gerenciamento de serviços. O prazo não começará a correr para chamados abertos que excedam a capacidade de atendimento contratada de 1 (uma) avaliação mensal. Na hipótese de detectar achados críticos, conforme pedido da Contratante, a contratada deverá emitir uma notificação imediata para os responsáveis pelo sistema avaliado imediatamente, independentemente do prazo do relatório. O serviço será avaliado em termos de tempestividade ao finalizar a entrega do relatório de teste conforme os prazos delimitados a seguir:

7.19.3.4. Clareza: O serviço será avaliado em termos de clareza pelo relatório de análise elaborado ao final de cada teste de invasão. A explicação dos achados deve permitir aos desenvolvedores a compreensão do erro e saber exatamente como corrigi-lo. Como instrumento de medição, pedidos de correção sem custos, ou potencial condição para a glosa será utilizado o número de retrabalhos necessários por conta de resultados insuficientemente documentados e que necessitem de mais esclarecimentos.

7.19.3.5. Relevância: O serviço será avaliado em termos de relevância ao respeitar a metodologia de priorização indicada a seguir:

7.19.3.5.1. Materialidade (M) de um módulo de código fonte: medido pelo número de linhas de código fonte efetivas (SLOC), tal como calculado por ferramentas como o SLOC count. Quando calculado como razão entre o número de SLOCs de um módulo e o número de SLOCs total do projeto, obtém-se a Materialidade Relativa (MR) do módulo de código fonte.

7.19.3.5.2. Nível de Risco (NR) de um módulo de código fonte: medido pelo número de hipóteses de vulnerabilidades testes definidos na agenda de teste que seriam investigados no módulo sob análise. Quando calculado como razão entre o Nível de Risco de um módulo e a soma do Nível de Risco de todos os módulos, obtém-se o Nível de Risco Relativo (NRR) do módulo de código fonte.

7.19.3.5.3. Nível de Prioridade (NP) de um módulo de código fonte: medido como o produto da MR e NRR do módulo. O Nível de Prioridade Relativa (NPR) será a razão entre o NP e a soma dos NPs de todos os módulos do projeto.

7.19.3.5.4. Dessa forma, o tempo disponibilizado para o escopo da análise seria distribuído de forma ponderada entre os módulos do projeto de acordo com o NPR de cada módulo.

7.19.4. A fiscalização técnica do serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (subitem 5 da tabela 1.2) avaliará os critérios de fiscalização com base nos documentos produzidos de modelo de ameaças e relatórios de análises de risco da seguinte forma:

7.19.4.1. Suficiência: O instrumento de medição adotado será Checklists ou Planilhas de Acompanhamento para apurar:

7.19.4.1.1. Se o modelo de ameaças conta com uma enumeração razoável de ameaças para todos os ativos afetados pelas novas soluções;

7.19.4.1.2. Se o modelo de ameaças contempla os controles já implementados que buscam mitigar as ameaças cogitadas;

7.19.4.1.3. Se as ameaças tiveram a sua probabilidade mensurada;

7.19.4.1.4. Se as ameaças tiveram os seus impactos coletados pelas equipes interessadas.

7.19.4.1.5. Se o relatório de ameaças contempla a descrição das ameaças que estipularam um risco inaceitável, descrevendo controles sugeridos para reduzir o risco no que for possível;

7.19.4.1.6. Se há acompanhamento e diálogo com a equipe interessada pela avaliação de risco.

7.19.4.2 Qualidade: A prestação do serviço será considerada de qualidade caso o relatório de análise de risco responda claramente às seguintes perguntas:

7.19.4.2.1. Quais são os cenários de ameaça identificados?

7.19.4.2.2. Quais controles já estão implementados?

7.19.4.2.3. Qual a probabilidade da ameaça se consolidar?

7.19.4.2.4. Quais são riscos inaceitáveis quando calculados os valores de risco?

7.19.4.2.5. Quais os controles sugeridos capazes de reduzir o risco das ameaças enumeradas?

7.19.4.2.6. Quais riscos foram diagnosticados como inaceitáveis?

7.19.4.3. Tempestividade: Como instrumentos de medição serão utilizadas as datas e horários imputados em eventos de baixa e entrega no sistema interno do órgão de gerenciamento de serviços. O prazo não começará a correr para chamados abertos que excedam a capacidade de atendimento contratada de 1 (uma) avaliação a cada seis semanas. O serviço será avaliado em termos de tempestividade ao finalizar a entrega do relatório de teste conforme os prazos delimitados a seguir:

7.19.4.3.1. As atividades de coleta de informações e de modelagem de ameaças devem ser realizadas em um período de 2 (duas) semanas, iniciados desde a reunião inicial de apresentação da solução.

7.19.4.3.2. A atividade de mensuração de riscos deve ser realizada em um período de 2 (duas) semanas iniciados desde o término da elaboração do modelo de ameaças.

7.19.4.3.3. A elaboração do relatório inicial resultante da avaliação de risco e da proposta de plano de ação deve ser realizado em um período de 2 (duas) semanas desde o término da mensuração de riscos.

7.19.4.3.4 Clareza: O serviço será considerado claro caso o relatório de avaliação de risco resultante seja apresentado de forma organizada, lógica e compreensível. A descrição das ameaças deverá ser objetiva e não conter ambiguidades que possam levar a interpretações erradas ou retrabalho.

7.19.4.3.5. Relevância: O serviço não será penalizado por sugestões de ameaças enumeradas ou por controles sugeridos além do necessário, exceto se enumerados em grandes quantidades que impossibilitem a sua utilização e leitura em tempo hábil. A relevância do serviço será avaliada em termos dos cenários de ameaça levantados na modelagem de ameaça. Os cenários terão a sua pertinência avaliada em termos de:

7.19.4.3.5.1. Criticidade dos ativos envolvidos;

7.19.4.3.5.2. Histórico de incidentes;

7.19.4.3.5.3. Tendências atuais de ataque divulgados na mídia;

7.19.4.3.5.4. Viabilidade e efetividade dos controles sugeridos para reduzir o risco das ameaças.

7.20. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

7.21. A tabela a seguir sintetiza a quantidade de itens avaliados por critério por serviço:

Subitem de Serviço da tabela do item 1.2	Suficiência (S)	Qualidade (Q)	Clareza (C)	Relevância (R)
1	Nº de pedidos de correções de vulnerabilidades realizados na semana (5 /semana, ajustado caso tenha feriados).	Nº de perguntas respondidas adequadamente nos pedidos de correções de vulnerabilidades (7 perguntas)	Número de retrabalhos de atos de comunicação que tenha resultado em disrupção de operações do órgão.	Nº de fatores de priorização (5 fatores de prioridade)
2 e 4	Nº de conteúdos ausentes no relatório de resultado do teste (3 tópicos)	Nº de perguntas respondidas com o relatório (6 perguntas)	Número de retrabalhos de atos de comunicação que tenha resultado em disrupção de operações do órgão.	Nº de fatores de priorização (3 fatores de prioridade)
3	Nº de hipóteses de vulnerabilidades analisadas (7 hipóteses)	Nº de perguntas respondidas com o relatório (6 perguntas)	Número de retrabalhos de atos de comunicação que tenha resultado em disrupção de operações do órgão.	Nº de fatores de priorização (3 fatores de prioridade)

5	Nº de hipóteses de vulnerabilidades analisadas (6 hipóteses)	Nº de perguntas respondidas com o relatório (6 perguntas)	Número de retrabalhos de atos de comunicação que tenha resultado em disrupção de operações do órgão.	Nº de fatores de priorização (4 fatores de prioridade)

7.22. Os fatores de avaliação de critérios S, Q, T, C e R são definidos a seguir:

7.22.1. Fator de Suficiência (S): A razão entre o número de itens entregues e o número total de itens previstos para o período.

7.22.2. Fator de Qualidade (Q): A razão entre o número de perguntas respondidas adequadamente pelo produto do serviço e o total de perguntas aplicáveis.

7.22.3. Fator de Tempestividade (T): 1 menos a razão entre o número de dias de atraso e a tolerância de atraso (5 dias). Não será utilizado para fins de glosa. Caso exceda a margem de tolerância, será adotado como critério para a aplicação de multa moratória, exceto para a prestação do serviço de gestão de vulnerabilidades (subitem 1 da tabela 1.2).

7.22.4. Fator de Clareza (C): 1 menos a razão entre o número de retrabalhos e a tolerância de retrabalhos (3).

7.22.5. Fator de Relevância (R): A razão entre o número de características utilizadas como critério de priorização dividido pelo número de características definidas para o serviço de priorização.

7.22.6. Os valores calculados para os fatores são então truncados para valores fixados como na tabela a seguir:

7.23. Os fatores de avaliação serão utilizados como métricas para a confecção dos termos de recebimento provisório e registrados no histórico de gerenciamento do contrato.

Valor calculado de Fator de Avaliação	Valor truncado do Fator de Avaliação
0%	0
1-20%	0,2
21-40%	0,4
41-60%	0,6
61%-80%	0,8
81-100%	1

7.24. A fiscalização técnica do serviço contínuo de testes de invasão (subitem 2 da tabela 1.2) e do uso do banco de horas de testes de invasão (subitem 4 da tabela 1.2) avaliará a conformidade e vigência de licença de uso corporativo de ferramenta de IA que visa assistir os testes a serem realizados. A comprovação deverá ser realizada antes da emissão da ordem de serviço inicial, demonstrando a disponiblidade e regularidade do licenciamento da ferramenta.

Fiscalização Administrativa

7.25. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.26. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Gestor do Contrato

7.27. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.27.1. coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço , do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.27.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.27.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.27.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.27.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.27.6. elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.27.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

7.27.8. receber e dar encaminhamento imediato:

7.27.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

7.27.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. Critérios de Medição e Pagamento

8.1. A avaliação da execução do objeto utilizará os instrumentos de avaliação de critérios especificados nas rotinas de fiscalização do contrato (seção 7.19).

8.2. Os serviços especializados especificados nos subitens 1, 2, 3 e 5 serão validados mensalmente de acordo com os requisitos especificados nas seções de Requisitos Técnicos no item 7.19.

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

8.3.1. não produziu os resultados acordados,

8.3.2. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

8.3.3. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

8.4. A utilização do Instrumento de Medição de Resultado (IMR), não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

8.5. Não haverá cumulatividade de glosa por degradação do critério de avaliação de tempestividade (T) e multa moratória para o mesmo atraso do mesmo produto. O critério de avaliação de tempestividade não será utilizado para fins de glosa de valor e será utilizado exclusivamente para indicar condição de aplicação de sanção para aplicação de multa moratória.

8.6. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

8.6.1. Os critérios de Suficiência, Qualidade, Tempestividade, Relevância e Clareza, conforme definidos na seção 7.19, serão utilizados para aferir a corretude da execução contratual para fins de pagamento.

8.6.2. Será adotado como janela de medição mensal para o cálculo dos critérios de avaliação do mês M as ordens de serviço com encerramento no mês M. Dessa forma, glosas apuradas serão aplicadas na parcela de M. Caso haja parcela incontroversa, esta poderá ser faturada independentemente da discussão sobre a parcela controvertida, nos termos do art. 143 da Lei nº 14.133/2021.

8.6.3. O critério de suficiência aplica um fator multiplicativo. Dessa forma, no caso de o critério de suficiência ser comprometido em sua integralidade (i.e.: A Contratante não entregue nada do serviço previsto), o valor glosado previsto para a rubrica daquele serviço será de 100%.

8.6.4. O critério de tempestividade não será usado para compor o cálculo de IMR e portanto não será usado para fins de glosa. Entretanto, será utilizado como critério para aplicar sanções administrativas de multa moratória caso seja violada a margem de atraso de tolerância.

8.6.5. As gradações de glosa para cada critério são como listados na tabela a seguir:

8.6.6. A parcela a ser glosada de um serviço na prestação de um mês respeitará então a seguinte fórmula de IMR: PGi=Pi S (50% Q+20% C+30% R) ; sendo PGi o valor do Preço Glosado do i-ésimo serviço; Pi é o valor a ser pago no mês devido à prestação do i-ésimo serviço; Q, C, R e S são fatores de atendimento do serviço aos critérios descritos de Qualidade, Clareza, Relevância e Suficiência conforme descritos no item 7.21.

Critérios	Peso de glosa
Qualidade	50%
Clareza	20%
Relevância	30%

Recebimento

8.7. Os serviços serão recebidos provisoriamente, no prazo de 5 dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.8. O prazo para recebimento provisório será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.9. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.10. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

8.11. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.12. Para efeito de recebimento provisório, será considerado para fins de faturamento o período mensal.

8.13. Ao final de cada período/evento de faturamento:

8.13.1. o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

8.14. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

8.15. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.16. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.17. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.18. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.19. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.20. Os serviços serão recebidos definitivamente no prazo de 5 (cinco) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.20.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

8.20.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

8.20.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.20.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.20.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.21. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.22. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.23. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

8.24. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.24.1. Validação mensal de execução dos serviços de acordo com o que foi definido nos critérios de aceitação da Ordem de Serviço dos serviços contínuos de gestão de vulnerabilidades (subitem 1), testes de invasão (subitem 2), inspeção de código fonte (subitem 3) e modelagem de ameaças e mensuração de riscos cibernéticos (subitem 5).

Liquidação

8.25. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

8.26. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.27. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

I. o prazo de validade;
II. a data da emissão;
III. os dados do contrato e do órgão contratante;
IV. o período respectivo de execução do contrato;

V. o valor a pagar; e
VI. eventual destaque do valor de retenções tributárias cabíveis.

8.28. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.29. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

8.30. A Administração deverá realizar consulta ao SICAF para:

8.30.1. verificar a manutenção das condições de habilitação exigidas;

8.30.2. identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

8.33. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

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

Prazo de pagamento

8.35. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.36. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA, mantido pelo Instituto Brasileiro de Geografia e Estatística – IBGE, de correção monetária.

Forma de pagamento

8.37. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

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

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

8.39.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.40. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Antecipação de pagamento

8.41. A presente contratação não prevê antecipação de pagamento. Os pagamentos serão efetuados após a entrega do serviço.

Reajuste

8.42. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 24/04/2026.

8.43. Após o interregno de um ano, contado na forma da legislação aplicável, os preços iniciais serão reajustados mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação (ICTI), mantido pelo Instituto de Pesquisa Econômica Aplicada (IPEA), exclusivamente em relação às obrigações cuja execução ocorra após a implementação da anualidade.

8.44. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.45. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

8.46. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

8.47. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

8.48. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

8.49. O reajuste será realizado por apostilamento.

Cessão de Crédito

8.50. As cessões de crédito dependerão de prévia aprovação do Contratante.

8.50.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

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

8.50.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

8.50.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

8.51. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9. Sanções Administrativas

9.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 48 (quarenta e oito) horas úteis.	Multa de 1 % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 10 (dez) dias úteis.
		Após o limite de 10 (dez) dias úteis, aplicar-se-á multa de 10 (dez) % do valor total do Contrato.
		Advertência.

2	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10 (dez) % do valor total do Contrato.

9.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

9.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

9.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a. der causa à inexecução parcial do contrato;
b. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c. der causa à inexecução total do contrato;
d. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e. apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f. praticar ato fraudulento na execução do contrato;
g. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.4.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

9.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

9.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

9.4.4. Multa:

9.4.4.1. Os valores de Moratória, Multa e Compensação são estipulados respeitando os limites previstos na Lei 14.133 /2021 Artigo 156.

9.4.4.2. Moratória, para as infrações descritas no item “d”, de **1**% (**um** por cento) por dia de atraso injustificado sobre o valor da **parcela inadimplida**, até o limite de **10** (**dez**) dias úteis.

9.4.4.3. Compensatória, para as infrações descritas acima alíneas “**e**” a “**h**” de **10**% (**dez** por cento) a **30**% (**trinta** por cento) do valor da(s) parcela(s) afetada(s) pelo ato fraudulento.

9.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “**c**”, de **5**% (**cinco** por cento) a 1**0**% (**dez** por cento) do valor do contrato.

9.4.4.5. Compensatória, para a infração descrita acima na alínea “**b**”, de **10**% (**dez** por cento) a **15**% (**quinze** por cento) do valor da contratação.

9.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de **8**% (**oito** por cento) a **15**% (**quinze** por cento) do valor da parcela afetada.

9.4.4.7. Compensatória, para a infração descrita acima na alínea “**a**”, de **5**% (**cinco** por cento) a **12**% (**doze** por cento) do valor da contratação a ser dosada conforme:

9.4.4.7.1. Extensão da inexecução;

9.4.4.7.2. Prejuízos operacionais causados;

9.4.4.7.3. Dolo ou culpa grave;

9.4.4.7.4. Reincidência e histórico de execução contratual.

9.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

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

9.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será cobrada judicialmente.

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de 22 (vinte e dois) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

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

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

9.11. Na aplicação das sanções serão considerados:

9.11.1. a natureza e a gravidade da infração cometida;

9.11.2. as peculiaridades do caso concreto;

9.11.3. as circunstâncias agravantes ou atenuantes;

9.11.4. os danos que dela provierem para o Contratante; e

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

9.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conj untamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

9.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

9.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contados da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

9.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

9.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

9.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

10. Critérios de Seleção de Fornecedor

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Regime de Execução

10.2. O regime de execução do contrato será por Empreitada por Preço Global.

10.2.1. A escolha pelo regime de contrato por empreitada por preço global se justifica pelo ganho de sinergia do trabalho de profissionais de mesma empresa para oferecer um serviço de suporte à segurança da informação integral ao Banco Central, então diminuindo o risco de enfrentar silos de conhecimento e maior carga administrativa em coordenar profissionais de empresas diferentes.

Exigências de habilitação

10.3. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.4. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.5. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

10.6. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.7. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.8. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.9. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.10. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.11. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.12. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.13. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.14. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.15. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.16. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.17. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.18. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

10.19. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.20. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.21. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis do último exercício sociai, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

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

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

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

10.22. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, **patrimônio líquido mínimo** de **10%** do **valor total estimado da contratação**.

10.23. Os indicadores fixados acima deverão ser atingidos no exercício social exigido para comprovação da qualificação econômico-financeira, sob pena de inabilitação;

10.24. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.25. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.26. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

Qualificação Técnica

10.27. O fornecedor deverá apresentar declaração de que tomou conhecimento de todas as informações e das condições necessárias ao cumprimento das obrigações objeto da contratação.

10.27.1 A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação

10.28. Registro ou inscrição da empresa na entidade profissional competente em plena validade;

10.28.1. Sociedades empresárias estrangeiras atenderão à exigência por meio da apresentação, no momento da assinatura do contrato ou do aceite de instrumento equivalente, da solicitação de registro perante a entidade profissional competente no Brasil.

10.29. O fornecedor deverá comprovar aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

10.29.1. Para fins de comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

10.29.1.1. Contrato(s) que comprove(m) a experiência mínima de 1 ano do fornecedor na prestação dos serviços, em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes;

10.29.1.2. Serão considerados válidos atestados relativos à prestação, de modo satisfatório, de serviços de segurança da informação. Assim sendo, o fornecedor deverá demonstrar experiência anterior na prestação continuada de serviços por período mínimo de 12 (doze) meses em pelo menos 2 (dois) dos 4 (quatro) serviços constantes no objeto desta contratação (isto é: serviço contínuo de gestão de vulnerabilidades, serviço contínuo de testes de invasão (pentesting), serviço contínuo de inspeção de código fonte e serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos);

10.29.1.3 Os meios de comprovação de experiência e de rotinas realizadas poderão ser contratos e cartas de declaração de contratantes pretéritos.

10.29.1.4. A experiência considerada válida para fins de comprovação da capacidade técnico-operacional deverá ter sido adquirida na prestação de serviços de segurança cibernética, segurança da informação ou operações correlatas em ambientes de missão crítica ou infraestruturas críticas, assim entendidos aqueles cuja interrupção, degradação, comprometimento ou indisponibilidade possa ocasionar impactos relevantes à continuidade de serviços essenciais, à segurança institucional, à estabilidade econômica ou à sociedade.

10.29.1.4.1. Para fins de aferição da compatibilidade da experiência exigida, serão considerados aptos os serviços executados em organizações que operem infraestruturas críticas ou ambientes de criticidade equivalente ou superior aos observados em instituições financeiras classificadas como S1 ou S2, em Instituições Operadoras de Infraestruturas do Mercado Financeiro (IOSMF), no Banco Central do Brasil, ou em outras organizações cuja operação exija elevados padrões de disponibilidade, resiliência operacional, continuidade de negócios, gestão de riscos cibernéticos e resposta a incidentes. **[1]**

10.29.1.4.2. A equivalência de complexidade técnico-operacional poderá ser demonstrada mediante documentação que evidencie a atuação da licitante em ambientes caracterizados por requisitos elevados de disponibilidade dos serviços, operação contínua, proteção de ativos críticos, gestão de incidentes de segurança da informação e observância de controles de resiliência operacional compatíveis com a criticidade do objeto da contratação.

10.29.1.4.3. A presente exigência decorre da natureza estratégica das atividades desempenhadas pelo Banco Central do Brasil e da relevância de seus ativos tecnológicos para o funcionamento do Sistema Financeiro Nacional (SFN), cuja continuidade e resiliência constituem fatores essenciais para a estabilidade econômica do País.

10.29.1.4.4. Nos termos da Política Nacional de Segurança de Infraestruturas Críticas e da Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), o setor financeiro integra o conjunto das infraestruturas críticas nacionais, caracterizadas pelo potencial de gerar impactos significativos à sociedade, à economia e ao Estado em caso de interrupção ou comprometimento de seus serviços.

10.29.1.4.5. Nesse contexto, a presente contratação contribui para a implementação dos objetivos e diretrizes da Estratégia Nacional de Segurança de Infraestruturas Críticas, especialmente no que se refere ao fortalecimento da segurança cibernética e da resiliência das infraestruturas críticas, bem como ao incentivo à adoção de recursos, capacidades e procedimentos avançados de proteção cibernética pelos responsáveis por tais infraestruturas.

10.29.1.4.6. A exigência não tem por finalidade restringir a competição a determinado segmento econômico, mas assegurar que a futura contratada possua experiência comprovada em ambientes submetidos a condições de criticidade compatíveis com aquelas verificadas no Banco Central do Brasil, caracterizados por elevados requisitos de disponibilidade, continuidade operacional, gestão de riscos cibernéticos, proteção de ativos críticos e pronta resposta a incidentes.

10.29.1.4.7. A medida constitui mecanismo de mitigação de riscos contratuais e operacionais, uma vez que a atuação em ambientes de missão crítica demanda maturidade organizacional, processos consolidados, experiência prática em cenários de alta complexidade e capacidade de resposta compatível com as consequências decorrentes de falhas de segurança ou interrupções de serviço.

10.29.1.4.8. Tal entendimento encontra respaldo nas diretrizes da Estratégia Nacional de Segurança de Infraestruturas Críticas, que reconhece o papel da Administração Pública na promoção da resiliência das infraestruturas críticas, inclusive por meio do estímulo à adoção de medidas de redução de riscos, do fortalecimento das capacidades de segurança cibernética e da prevenção de eventos capazes de gerar impactos

econômicos, sociais e institucionais expressivos ou demandar a aplicação de significativos recursos públicos para recuperação dos serviços afetados.

10.29.2. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante.

10.29.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.29.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

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

10.29.6. A Administração poderá solicitar documentos complementares para verificação da autenticidade dos atestados apresentados, incluindo cópia de contratos, informações de contato do emitente e descrição detalhada dos serviços executados.

10.29.7. Para a comprovação de experiência mínima, é preciso comprovar que a empresa para a qual os serviços tenham sido prestados pelo fornecedor tenha porte de no mínimo 4500 ativos, equivalente a 50% do porte do BCB.

10.30. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.31. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

Disposições gerais sobre habilitação

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

10.33. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

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

Critérios de Presunção de Inexequibilidade

10.35. Será considerada presumidamente inexequível (presunção relativa) a proposta que apresentar um ou mais subitens dotados de valor proposto inferior a 50% (cinquenta por cento) do seu respectivo valor estimado, o qual foi estabelecido com base na pesquisa de preços constantes no Estudo Técnico Preliminar (ETP).

10.35.1. O critério adotado fundamenta-se, por analogia, no art. 59, §4º, da Lei nº 14.133/2021, bem como nas orientações do Tribunal de Contas da União, emanadas do Acórdão nº 2.362/2015.

10.35.2. A aplicação da presunção de inexequibilidade por subitem decorre da natureza tecnicamente autônoma e economicamente individualizável de cada serviço, os quais possuem insumos, composição de custos e equipes distintas, não sendo possível compensação econômica entre eles sem prejuízo à adequada execução contratual.

10.36. A análise de exequibilidade será realizada por subitem, podendo a proposta ser desclassificada caso reste comprovada a inviabilidade de execução de qualquer dos subitens, ainda que os demais se mostrem exequíveis.

10.37. A presunção de inexequibilidade poderá ser afastada mediante comprovação, pela LICITANTE classificada em primeiro lugar, da viabilidade econômica e operacional da proposta.

10.37.1. A comprovação deverá ser realizada por meio da apresentação de documentos relativos à execução anterior, de modo satisfatório, de contratos compatíveis com o objeto, contendo evidências suficientes para demonstrar a capacidade de execução nas condições ofertadas.

10.37.2. Serão aceitos um ou mais contratos, cuja análise conjunta permita aferir a exequibilidade da proposta.

10.37.3. A Administração avaliará os documentos apresentados com base nos seguintes critérios:

I – Compatibilidade de preços: demonstração de execução de serviços com valores proporcionais ao da proposta apresentada, admitidos os devidos ajustes monetários por índices oficiais;

II – Compatibilidade técnica: comprovação de emprego de equipe com qualificação e dimensionamento compatíveis com o objeto;

III – Compatibilidade operacional: evidências de execução de serviços de natureza semelhante, em volume e complexidade equivalentes;

IV – Qualidade da execução: demonstração de cumprimento satisfatório de níveis de serviço, quando aplicáveis.

10.37.3.1. Para um contrato apresentado como evidência de exequibilidade de proposta ser aceito, serão aplicados os seguintes critérios:

10.37.3.1.1. O valor dos serviços prestados, para cada subitem sob análise, deverá ser menor ou igual ao preço ofertado no pregão.

10.37.3.1.1.1. O valor do contrato deverá ser reajustado pelo índice de ICTI desde o momento da assinatura até o mês da apresentação da documentação de comprovação de exequibilidade.

10.37.3.1.1.1.1. Esta exigência é colocada para que os valores estejam na mesma base de comparação da contratação referente a este TR.

10.37.3.1.1.2. Para cada subitem a ter sua exequibilidade comprovada, deverá ser apresentado um contrato indicando compatibilidade de preços.

10.37.3.1.1.2.1. Caso um mesmo contrato inclua a prestação de dois ou mais serviços que serão utilizados para comprovar a exequibilidade de dois ou mais subitens do termo de referência, será admitido o uso de um mesmo contrato para comprovação de exequibilidade de vários subitens. Entretanto, será necessário decompor o preço global do contrato em componentes proporcionais ao número de profissionais utilizados para prestar os serviços sob comprovação.

10.37.3.2. Disposições sobre a avaliação do corpo técnico utilizado:

10.37.3.2.1. Apenas contratos que tenham empregado um corpo técnico em conformidade com os requisitos técnico-profissionais deste objeto serão aceitos para comprovação de exequibilidade de cada subitem sob análise.

10.37.3.2.1.1. Para o “Subitem 1 – Serviço contínuo de gestão de vulnerabilidades”, a conformidade será verificada com base na capacitação profissional definida no subitem 4.22.

10.37.3.2.1.2. Para os “Subitem 2 – Serviço contínuo de testes de invasão (pentesting)” e “Subitem 4 - Banco de Horas de Pentest”, a conformidade será verificada com base na capacitação profissional definida no subitem 4.23.

10.37.3.2.1.3. Para o “Subitem 3 – Serviço contínuo de inspeção de código fonte”, a conformidade será verificada com base na capacitação profissional definida no subitem 4.24.

10.37.3.2.1.4. Para o “Subitem 5 – Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos”, a conformidade será verificada com base na capacitação profissional definida no subitem 4.25.

10.37.3.2.2. É preciso apresentar a lista de profissionais que prestaram os serviços mencionados no contrato com a respectiva discriminação de informações:

10.37.3.2.2.1. Data de início e fim de prestação de serviço de cada profissional;

10.37.3.2.2.2. Quantidade de horas efetivamente executadas por cada profissional;

10.37.3.2.2.3. Comprovação de vínculo do profissional com a licitante no período;

10.37.3.2.2.4. Currículo de cada profissional à época da prestação do serviço;

10.37.3.2.3. Somente serão considerados aceitos para contabilização do volume dos perfis profissionais exigidos aqueles que apresentem perfil em conformidade o demandado para os perfis de analista de segurança da informação sênior.

10.37.3.3. Para cada subitem sob análise, é preciso apresentar evidências de prestação de serviços em volume compatível com o estipulado neste termo de referência.

10.37.3.3.1. Serão aceitos somente contratos de vigência igual ou superior a 1 (um) ano de prestação de serviços de segurança da informação de forma ininterrupta e sem intercorrências;

10.37.3.3.1.1. Em caso de interrupções ou intercorrências, só serão considerados para cálculo de 1 (um) ano de prestação de serviços a vigência total do contrato descontados os períodos de interrupções ou intercorrências.

10.37.3.4. É preciso apresentar evidências de que a prestação dos serviços relativos aos subitens sob análise se deu mediante a utilização de ordens de serviços que foram submetidas a apuração de níveis mínimos de serviço ou métrica similar.

10.37.3.4.1. Em caso de contratos com a administração pública, poderá ser usada como evidência a declaração da área gestora do contrato no órgão emissor do atestado que confirme que os níveis mínimos de serviço foram apurados e que a licitante atingiu as metas em todo o período a que se refere tal atestado.

10.38. A decisão sobre a exequibilidade será motivada, com base nos elementos apresentados e nos critérios definidos neste Termo de Referência.

10.38.1. Deverão ser apresentados contratos, aditivos e documentos auxiliares referentes a experiências de prestação de serviço passadas pela LICITANTE.

[1] A classificação de tipo de instituição de financeira é disponibilizada no site https://www.bcb.gov.br/estabilidadefinanceira/sistemasautorizados_spb

11. Estimativas do valor da contratação

11.1. O custo estimado total da contratação, é de R$ 12.091.369,03 (Doze milhões e noventa e um mil e trezentos e sessenta e nove reais e três centavos), conforme custos unitários apostos na tabela da seção 1.1 deste TR.

12. Adequação orçamentária

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União e no Orçamento da Autoridade Monetária.

12.2. A contratação será atendida pela seguinte dotação, com distribuição prevista de 42% do valor atendido pela OAM e 58% atendido pela OGU:

1. **OGU E OAM**		
Função Programática		**Plano de Trabalho Resumido - PTRES**
04.125.4103.21B1.0001		232523
Código	**Conta**	**Natureza**
40.10.1.001-5 (OAM)	3990.10.03-1	
40.10.2.005-0 (OGU)	4030.36.03-5	339040

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

12.4. A distribuição das despesas referentes a este projeto entre o OAM e o OGU se justifica pelo fato dos serviços de segurança especializados contratados cobrirem como objeto os sistemas corporativos internos e os sistemas de sustentação de sistemas de pagamentos como o PIX.

13. Disposições finais

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas .

14. Responsáveis

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

FELIPE KENZO SHIRAISHI

Integrante Técnico

Assinou eletronicamente em 13/11/2026 às 14:54:22.

DANILO DIAS

Integrante Requisitante

IURI SOUSA DA ROCHA

Integrante Administrativo

Despacho: Considerando que as informações inseridas neste processo apresentam as justificativas para a contratação pretendida e os benefícios a serem alcançados, aprovo este documento.

OCTAVIO DO VALE ROCHA

Autoridade competente

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Doc 23 - Anexo 1 - Exemplos numericos de calculo do preco glosado - Retificado.pdf (200.03 KB)
- Anexo II - Doc 24 - Anexo 2 - Termo de compromisso de manutencao de sigilo - TCMS - Retificado.pdf (153.65 KB)
- Anexo III - Doc 45 - Anexo 3 - Modelo de Termo de Ciencia e Compromisso das Normas de Seguranca do Banco Central.pdf (70.47 KB)