BANCO CENTRAL DO BRASIL - BRASÍLIA

Estudo Técnico Preliminar 30/2026

1. Informações Básicas

Número do processo: 305279

2. Descrição da necessidade

Nesta seção é descrita a necessidade motivadora para contratação de serviço especializado de segurança da informação para o BCB. A seguir, é apresentado o problema institucional enfrentado, causas e agravantes para os problemas apresentados, o impacto de não mitigação do problema, a caracterização das necessidades institucionais e o vínculo com os instrumentos estratégicos vigentes para a instituição.

2.1. PROBLEMA INSTITUCIONAL

O Banco Central do Brasil possui um inventário diverso de soluções de TIC. Estas soluções são ou contratadas ou desenvolvidas internamente. Para ambos os casos, há procedimentos de segurança cibernética que precisam ser realizados nestes sistemas em dois momentos distintos: quando já implantados e quando serão implantados.

Para sistemas já implantados, estes podem estar expostos a novas vulnerabilidades descobertas ou vulnerabilidades já conhecidas, mas ainda não detectadas. Dessa forma, é necessário aplicar o procedimento de gestão de vulnerabilidades para detectar a presença de vulnerabilidades no ambiente de forma tempestiva e avaliar a urgência em acionar a sua correção pela equipe de manutenção responsável com base em critérios de explorabilidade, exposição e criticidade do sistema para a missão institucional do BCB. Este processo enfrenta dois desafios: um interno e outro externo. O desafio interno diz respeito ao tamanho e complexidade da atual infraestrutura tecnológica do BCB. O desafio externo diz respeito ao atual cenário de ameaças cibernéticas relacionadas à crescente descoberta e publicações de vulnerabilidades que vulneram ativos de TIC empregados neste ambiente do BCB.

Para sistemas a serem implantados, a nova solução pode expor a instituição a novos riscos. Antes de serem disponibilizados, há a necessidade de implantar controles para mitigar os seus riscos. Conforme definido no manual de Procedimentos Operacionais de Segurança em TI do BCB (POSTI), é prevista uma análise de vulnerabilidade nos serviços antes de entrarem em produção. Com a vazão de lançamentos de serviços internos e de implantação de novas soluções de terceiros, a fila de análises torna-se extensa. Caso a área de segurança cibernética não apresente uma vazão adequada para estas análises, a área pode tornar-se um gargalo processual, comprometendo prazos de entrega de serviços públicos ofertados pela instituição. Dentre estas análises, é possível enumerar os testes de segurança (caixa-preta ou caixa-branca) e avaliações de risco.

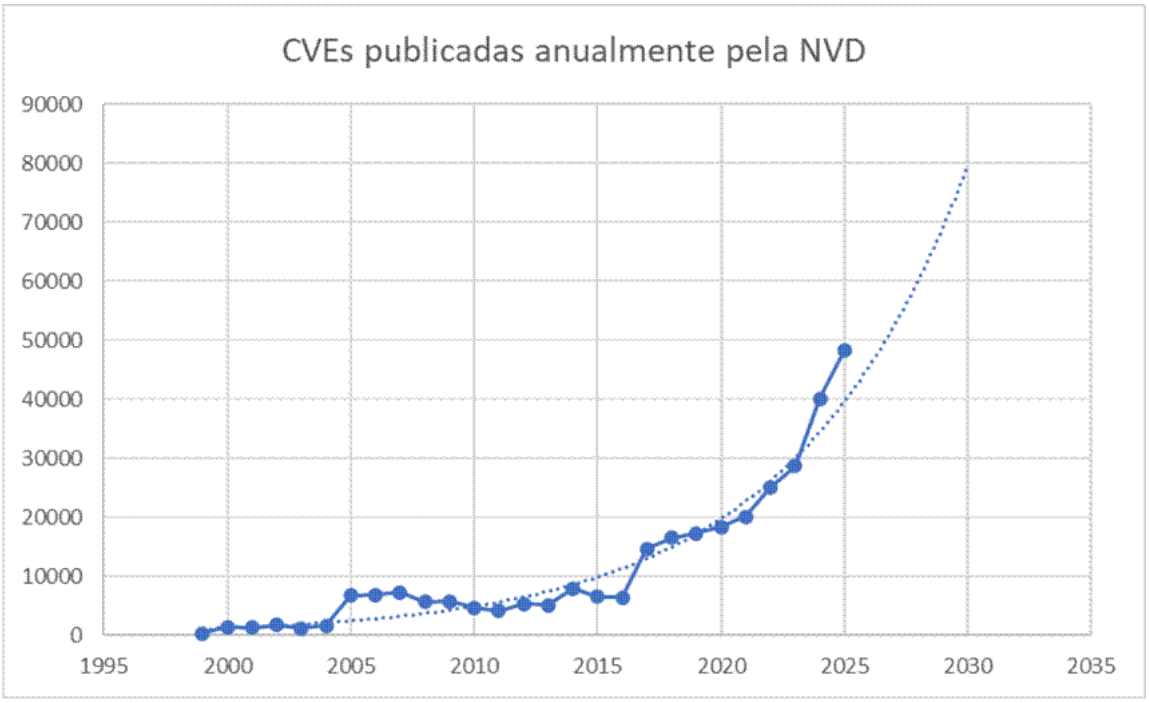
Atualmente, com o quadro funcional disponível, o acompanhamento e tratamento destes esforços de gestão de vulnerabilidade e análises de segurança enfrentam limitações, uma vez que tais atividades competem com outras atribuições funcionais deste quadro já reduzido.

2.2. CAUSAS E AGRAVANTES

Quantificando o desafio interno, atualmente, o Banco Central do Brasil monitora mais de 9.000 ativos de TI e mais de 6000 softwares distintos (sendo aplicações ou pacotes de dependência). Para além dos ativos de TI, há uma base de código de mais de 1600 projetos de código fonte de soluções internas, cada uma com um conjunto de dependências externas. Tais projetos culminam em mais de 1200 imagens de container em ambiente de produção. Esta heterogeneidade e dimensão do cenário de TIC do BCB expressa a complexidade do ambiente em termos de gestão de segurança.

Com a quantidade de projetos atualmente desenvolvidos e que aguardam análise de segurança para serem publicados em produção e a projeção de novos projetos para 2030, é prevista uma demanda consistente por análises de segurança que reflita a demanda atendida nos últimos 4 anos. Esta demanda se traduz na revisão de 24 soluções novas sendo implantadas por ano.

Quantificando o desafio externo, de acordo com os dados de série histórica de CVEs publicadas anualmente no NVD do NIST [1], há uma evolução exponencial de publicações com capacidade de alcançar a marca de 80.000 vulnerabilidades publicadas até 2030, conforme apresentado no gráfico abaixo.



Dessa forma, foi possível verificar que, para o ano de 2025, haveria um total de 132 vulnerabilidades publicadas por dia, com a extrapolação para 2030 chegando a valores de 225 vulnerabilidades diárias. Para estimar o quanto estas projeções se traduziriam em esforço de gerenciamento no Banco Central, foi calculado um Fator de Conversão composto pela multiplicação de taxas atenuadoras de esforço de gerenciamento. Dentre as premissas utilizadas para compor as taxas de atenuação constam a existência de ferramentas instaladas no ambiente para gerenciamento de

vulnerabilidades, a taxa de priorização, que considera o percentual de CVEs publicadas que apresentam severidade alta ou crítica e o fato de haver softwares gerenciados, que são submetidos a correções de segurança automatizadas no ambiente, como navegadores e sistemas operacionais.

Com o atenuador da existência de ferramentas disponíveis para inventariar ativos, monitorar a sua exposição a vulnerabilidades e ter canais de atualização remota de softwares em servidores e estações de trabalho, considerou-se uma taxa de atenuação de esforço de 25%. De acordo com o cálculo de distribuição de CVSS por CVEs realizado em [2], 56% das CVEs publicadas são de severidade alta ou crítica. Finalmente, considerou-se, arbitrariamente, uma taxa de 25% de CVEs que afetem os 6.000 softwares instalados no BCB. Com isso, multiplicando tais taxas de atenuação, foi possível chegar a um fator de conversão de esforço diário de 3,5%.

Como resultado, o esforço previsto de gerenciamento de vulnerabilidades do BCB representa, no mínimo, um total de 5 vulnerabilidades por dia com a possibilidade de escalar para 8 vulnerabilidades diárias até 2030, conforme ilustrado no gráfico abaixo.



Cabe apontar que o gerenciamento de vulnerabilidades não se limitaria a tratar somente vulnerabilidades publicadas recentemente, mas também tratar vulnerabilidades existentes em sistemas legados.

Dessa forma, ficam caracterizadas as causas e agravantes em termos quantitativos sobre as necessidades do BCB.

2.3. IMPACTOS DA NÃO AÇÃO

A não resolução dos problemas acima descritos tem capacidade de comprometer a resiliência cibernética do BCB. Isto significaria expor a instituição a 2 (dois) riscos principais: (1) ao risco de submeter a sua infraestrutura tecnológica a uma janela de exposição a ameaças cibernéticas externas em duas dimensões: por tempo em que as vulnerabilidades se encontram não corrigidas, e pelo número de softwares com vulnerabilidades. Além disso, (2) também expõe a instituição ao risco de atraso em suas entregas de serviços mediados por TI oferecidos pela instituição. Em conclusão, fica caracterizada a necessidade de complementação da força de trabalho do BCB para endereçar os seus desafios de gestão de vulnerabilidades.

2.4. NECESSIDADE INSTITUCIONAL

Para resolver o problema descrito, 5 necessidades são identificadas:

- Suporte contínuo em gestão de vulnerabilidades;
- Suporte em testes de invasão (pentests);
- Suporte em inspeção de código fonte;
- Suporte em modelagem de ameaças e mensuração de riscos;
- Elasticidade operacional para pentest.

2.5. RELAÇÃO COM INSTRUMENTOS ESTRATÉGICOS

O Plano Direto de Tecnologia da Informação e Comunicação do BCB - PDTIC 2020-2025 [19], em seu capítulo 6, enumera objetivos estratégicos para a governança de TIC da instituição. Dentre estes objetivos, destacam-se 2:

- OE 1 - Aprimorar a governança, os processos internos e a gestão dos recursos de TIC;
- OE 7 - Promover segurança cibernética e privacidade digital.

Atendendo ao objetivo OE 7, estas atividades são realizadas pela área requisitante DISEG/SETIR:

- Monitoramento e análise de vulnerabilidades em ativos de TIC, denominado internamente de Gestão de Ameaças e Vulnerabilidades (GAV);
- Avaliações de risco de ativos de TIC, em um processo interno denominado de Programa de Mensuração e Avaliação de Riscos Cibernéticos (PMARC).

Buscando atender ao objetivo OE 1 com eficiência e efetividade orientado ao objetivo OE 7, a área requisitante descreveu a necessidade desta contratação.

Além disso, a contratação proposta atende diretamente ao interesse público ao assegurar a continuidade, confiabilidade e segurança dos serviços essenciais prestados pelo Banco Central do Brasil ao Sistema Financeiro Nacional e à sociedade. A crescente complexidade do ambiente tecnológico do BCB, somada à evolução acelerada das vulnerabilidades e ameaças cibernéticas, exige capacidade técnica especializada para identificar, analisar e mitigar riscos de forma tempestiva.

A ausência desse suporte pode resultar em indisponibilidade ou comprometimento de serviços críticos, como plataformas de pagamentos, liquidação, supervisão e demais sistemas estruturantes, afetando a estabilidade do Sistema Financeiro Nacional (SFN) e a prestação de serviços ao cidadão e às instituições reguladas.

Assim, a contratação contribui para a proteção da infraestrutura crítica sob responsabilidade do BCB, fortalece a resiliência cibernética institucional e assegura a adequada entrega das políticas públicas monetárias, financeiras e de pagamentos. Trata-se, portanto, de medida necessária para preservar o interesse coletivo, a segurança econômica do país e a confiança da sociedade nas funções desempenhadas pelo Banco Central.

2.6. RESUMO DAS NECESSIDADES

Diante do exposto, evidencia-se a necessidade de contratar serviços especializados para suprir lacunas operacionais, manter a resiliência cibernética do BCB e evitar riscos de continuidade e integridade de serviços essenciais. Dessa forma, sintetiza-se a comparação entre a situação atual, a capacidade desejada e o hiato identificado que a solução busca suprir no seguinte quadro resumo:

Estado atual	Capacidade desejada	Hiato identificado
Há uma demanda corrente de 2 (dois) testes de invasão por mês.	Ter capacidade de vazão de (2) dois testes de invasão por mês	Limitação de capacidade operacional interna de número de servidores
Há eventual demanda adicional e imprevisível por mais análises de vulnerabilidades.	Ter a capacidade de aumentar a capacidade de oferta de análise de vulnerabilidades com elasticidade.	Limitação de capacidade operacional interna de número de servidores
Há uma necessidade por avaliação minuciosa da segurança dos sistemas codificados internamente.	Ter a capacidade de avaliar a segurança de um código fonte de projeto para encontrar vulnerabilidades que não seriam detectadas por um modelo caixa-preta.	Limitação de capacidade operacional interna, havendo somente 1 servidor realizando a avaliação.
Há uma demanda corrente de 1 avaliação de riscos mensal.	Ter a capacidade de vazão de realizar uma avaliação de risco por mês	Limitação de capacidade operacional interna de número de servidores
O ambiente apresenta uma grande quantidade de ativos expostos a novas vulnerabilidades descobertas diariamente e que precisam de notificações para correções.	Ter a capacidade de responder à publicação de vulnerabilidades que representem uma ameaça ao BCB diariamente.	Limitação de capacidade operacional interna de número de servidores

3. Área requisitante

Área Requisitante	Responsável
DEINF/INFRA/DISEG/SETIR	Danilo Dias

4. Necessidades de Negócio

Para superar os problemas identificados e garantir a continuidade e resiliência das operações do BCB, são necessárias as seguintes capacidades de negócio:

1. Ter a capacidade de, com precisão, monitorar a exposição de ativos de TIC inventariados do BCB a novas vulnerabilidades descobertas;
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;
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. Ter a capacidade de, continuamente, testar a efetividade das funcionalidades de segurança conforme codificado nas soluções internas do BCB.
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.

5. Necessidades Tecnológicas

Para atender às necessidades de negócio identificadas, a solução tecnológica a ser contratada deverá possuir as seguintes características mínimas:

5.1. DETECÇÃO E GESTÃO DE VULNERABILIDADES

O serviço deverá:

- Realizar o monitoramento contínuo de vulnerabilidades relacionadas aos softwares, componentes e serviços utilizados nos ambientes do BCB.
- Classificar e contextualizar vulnerabilidades com base no impacto específico ao ambiente institucional, indo além de métricas genéricas como CVSS.
- Permitir comunicação técnica precisa com as equipes responsáveis pela manutenção dos sistemas, incluindo descrição da vulnerabilidade, impacto, e recomendações de correção.
- Manter processos e interfaces seguras para inventário e gestão de exposição de ativos.
- Oferecer mecanismos de alerta tempestivos, com priorização automática baseada em critérios de severidade técnica e risco operacional.

5.2. TESTES DE INVASÃO

O serviço deverá:

- Disponibilizar capacidade de realização de testes de invasão sob demanda, abrangendo aplicações, serviços e infraestruturas.
- Execução de técnicas representativas de atacantes reais, incluindo vetores externos e internos, com cobertura de táticas e técnicas relevantes.
- Capacidade de adaptação de profundidade dos testes conforme complexidade e criticidade dos sistemas avaliados.
- Relatórios técnicos completos, contendo evidências, impacto, risco e recomendações de correção.
- Execução escalável, permitindo atender variações na demanda institucional sem afetar prazos de entrega operacional.

5.3. ANÁLISE MANUAL DE CÓDIGO FONTE

O serviço deverá:

- Prover serviço de análise manual especializada de segurança de código abrangendo vulnerabilidades de implementação, lógica de negócio e arquitetura.
- Capacidade de identificar fluxos de dados, dependências e comportamentos complexos, que não são detectados por análises automatizadas.
- Avaliação segura de múltiplas linguagens e frameworks, conforme adotado nos sistemas do BCB, priorizando Java-Spring, C#-.Net, Node.JS-angular e Python.
- Emissão de relatório detalhado, contendo diagnósticos, classificação, exploração possível, impacto e recomendações.
- Oferecer consultoria para desenvolvedores do BCB que precisarem tirar dúvidas sobre codificação segura e alertas de segurança emitidos por ferramentas de detecção de vulnerabilidades instalados em pipeline de CI/CD.

5.4. MODELAGEM DE AMEAÇAS E AVALIAÇÃO DE RISCOS

O serviço deverá:

- Realizar modelagem estruturada de ameaças para sistemas internos e de terceiros, incluindo soluções em nuvem.
- Identificar cenários de risco, atores de ameaça e vulnerabilidades estruturais, considerando aspectos técnicos e funcionais.
- Fornecer estimativas de risco cibernético com base na metodologia CIS-RAM v2.2.
- Recomendar controles mitigatórios adequados ao risco e ao ambiente do BCB.
- Apoiar avaliações extraordinárias conforme surgimento de novas soluções ou alterações arquiteturais relevantes.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

1. Para além dos requisitos de negócios e tecnológicos mencionados, é importante que a solução atenda aos seguintes requisitos:
2. Os profissionais responsáveis por prestar o serviço solicitado deverá atender a um desses requisitos:

1. ter experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em Segurança da informação;
2. ou possuir Mestrado ou Doutorado, com tema de pesquisa relacionado ao processo de segurança a ser prestado como serviço;
3. ou possuir pelo menos uma certificação avançada segundo o painel de certificações de segurança open-source de Paul Jerimy [60]:
    1. Para o serviço de gestão de vulnerabilidades, ter:
        1. Pelo menos uma das certificações a seguir: 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; ou
        2. Pelo menos duas das certificações a seguir: 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.
    2. Para o serviço de testes de invasão, ter pelo menos:
        1. Pelo menos, uma das certificações a seguir: 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; ou
        2. Pelo menos, duas das certificações a seguir: 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.
    3. Para o serviço de inspeção de código fonte, ter:
        1. Pelo menos uma das certificações a seguir: 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 II; ou
        2. Pelo menos duas das certificações a seguir: 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. Para o serviço de modelagem de ameaças e mensuração de riscos, ter:
        1. Pelo menos uma das certificações a seguir: GSE, CISSP Concentrations, CISM, S-ISME, CISSP, CCISO, EEXIN ISM, GSP, S-CISO, CASP+, CISSM, CRISC ou CGRC; ou
        2. Pelo menos, duas das certificações a seguir: 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.

Os serviços devem ser oferecidos por uma equipe integrada com possibilidade de diálogo e intercâmbio de informações, pois os insumos gerados por um processo serão utilizados em outro (e.g.: Os modelos de ameaça gerados pelo serviço de modelagem de ameaças e avaliação de riscos podem ser usados como documentação para os processos de pentest e inspeção de código fonte).

7. Estimativa da demanda - quantidade de bens e serviços

Nesta seção, é apresentada uma estimativa de demanda para as necessidades apresentadas anteriormente.

7.1. ESTIMATIVA DE DEMANDA – GESTÃO DE VULNERABILIDADES

Para atender à necessidade de gestão de ameaças e vulnerabilidades em ativos, estima-se a necessidade de endereçar 8 vulnerabilidades por dia (conforme as projeções apresentadas sobre a estimativa de esforço de gerenciamento de vulnerabilidades até 2030), com uma média de 1 hora de trabalho por vulnerabilidade endereçada (análise, priorização, abertura de solicitação e acompanhamento), indicando uma quantidade recomendada de prestação de serviço por 1 (um) analista dedicado.

7.2. ESTIMATIVA DE DEMANDA – TESTES DE INVASÃO

Atualmente, o Banco Central apresenta uma demanda efetiva mensal de pelo menos 2 (dois) testes de invasão mensalmente, com esforço estimado de 160 horas de trabalho por teste, em média, indicando uma quantidade recomendada de prestação de serviço por 2 (dois) analistas dedicados.

7.3. ESTIMATIVA DE DEMANDA – INSPEÇÃO DE CÓDIGO FONTE

A inspeção de código fonte é uma complementação de teste de caixa branca a ser agregado aos testes de invasão. Entretanto, nem toda solução objeto de teste de invasão no Banco Central trata-se de uma solução desenvolvida internamente. Dessa forma, estima-se uma quantidade de 1 (uma) inspeção por mês, com esforço estimado de 160 horas de trabalho por inspeção, em média, indicando uma quantidade recomendada de prestação de serviço por 1 (um) analista dedicado.

7.4. ESTIMATIVA DE DEMANDA – AVALIAÇÃO DE RISCOS

O Banco Central, em seu Programa de Mensuração e Avaliação de Riscos Cibernéticos (PMARCBC), estipula uma periodicidade de realizar 2 (duas) avaliações de riscos cibernéticos por ano. Entretanto, também estipula que toda solução a ser hospedada em nuvem precise ser submetida a uma avaliação de riscos. Com o aumento do número de soluções contratadas a serem hospedadas em nuvem, houve um aumento no número de avaliações de riscos extraordinárias, tornando-se parte de uma rotina que consiste em uma média de 8 avaliações por ano, com esforço estimado de 240 horas de trabalho por avaliação. Dessa forma, indica-se uma quantidade recomendada de prestação de serviço por 1 (um) analista dedicado.

8. Levantamento de soluções

Cada alternativa de solução é apresentada em seção dedicada discriminando o tipo considerado.

8.1. NECESSIDADES SIMILARES DE OUTROS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA

Em atendimento ao artigo 11º da IN SGD/ME nº 94/2022 [4], foi realizada pesquisa estruturada no PNCP com o objetivo de identificar soluções semelhantes e avaliar aderências e modelos de contratação praticados por outros órgãos. A consulta ao Portal Nacional de Compras Públicas (PNCP) foi realizada no dia 26 de janeiro de 2026 por termos relacionados às necessidades de negócios enumeradas de editais e datados de 1 ano de diferença. A seguir, resume-se o resultado destas buscas.

8.1.1. SERVIÇO DE INSPEÇÃO DE CÓDIGO FONTE

Realizou-se a busca pelos termos “Código Fonte”. Com isso, obteve-se 980 registros. Filtrando os casos procurando por menções aos termos “Inspeção” e “Auditoria”, obteve-se 0 registros. Buscando pelos termos “Revisão” e “Análise”, verificou-se cada um com um registro. Entretanto, ao avaliá-los, descobriu-se não pertinente, por não se tratar de casos de serviço de avaliação de segurança de código fonte como desejado. O caso retornado para o termo de filtro “Análise”, tratava-se de edital de contratação de serviço de fornecimento de código fonte no lugar de inspecioná-lo em termos de segurança da informação (Órgão: 04203025000143; Edital nº 1/2024 [20]). Para o caso retornado para o termo de filtro “Revisão”, tratava-se de um edital de registro de preços para realizar georreferenciamento de solo (Órgão: 27165745000167; Edital nº 25/2024 [21]). Usando o termo de busca “Auditoria” de filtro, obteve-se nenhum registro.

Dessa forma, conclui-se não haver referências de contratações similares realizadas por outros órgãos da administração pública para a necessidade de apoio à inspeção de segurança de código fonte. A inexistência de contratações similares referentes a inspeção de código fonte pode ser explicada pelo menor número de soluções tecnológicas desenvolvidas e mantidas internamente. Dada a diversidade de aplicações desenvolvidas pelo BCB (PIX, STR, SELIC, etc.) e o nível de criticidade e exposição, então se caracterizando como Infraestrutura Crítica conforme o Decreto nº 11.200/2022 [3], a necessidade por uma inspeção do código fonte de tais soluções se faz mais relativamente relevante do que em outros órgãos em que as soluções presentes em seu parque, em sua maioria, possam se tratar de soluções de terceiros.

8.1.2. SERVIÇO DE MODELAGEM DE AMEAÇAS E MENSURAÇÃO DE RISCOS

Realizou-se a buca pelos termos “Ameaça”, seguido de filtragem acompanhada do termo “Modelagem”, esta busca resultou em 0 registros. Também se realizou a busca de “Risco”, seguido de filtragem acompanhada do termo “Avaliação”. Esta sequência de busca retornou muitos casos não relacionados ao contexto de TIC, tendo que descartar os registros que contivessem termos como “socia”, “saúde”, “ambient”, uma vez que havia registros de contratação de serviço para tratar de assistência social de pessoas expostas a riscos ambientes ou de saúde. Ao descartar tais casos, obteve-se 14 registros. Entretanto, ao avaliar a descrição destes casos, apenas um aparentou ser pertinente. Ao avaliá-lo, concluiu-se que era um caso não pertinente por tratar-se de um caso de pentest. O serviço mencionado de avaliação de risco não é realizado em perspectiva preventiva, mas ad-hoc mediante a identificação e vulnerabilidades detectadas.

Dessa forma, conclui-se não haver referências de contratações similares realizadas por outros órgãos da administração pública para a necessidade de apoio a processos de modelagem de ameaças e avaliação de riscos.

8.1.3. SERVIÇO DE TESTES DE INVASÃO

Realizou-se a busca pelos termos “Pentest”, “Intrusão” e “Invasão”, tendo então um retorno de 8, 483 e 100 registros respectivamente. Filtrando cada um dos resultados procurando pela ocorrência do termo

“test”, verificou-se o retorno de 6, 4 e 4 registros respectivamente. Ao descartar as interseções entre as buscas, obteve-se 8 registros de pesquisa.

Destes itens, foram identificados como editais pertinentes e similares às necessidades do BCB os de número nº 90.078/2025 (CODEVASF) [22], nº 90.007(5)/2025 (FMABC) [23] e nº 90.088 (TJSP) [24]. Outros editais se diferenciam e são de difícil comparação por adotarem modelo de pentest de escopo único ou terem o seu preço sem distinção dos outros serviços de segurança contratados como é o caso dos editais de número n º 90.009/2025 (Aeroporto de Maricá) [25], nº 006/2025 (ARIS) [26] e nº 90.023/2025 (TJM-SP) [27].

Em síntese, outros órgãos públicos têm contratado o serviço de pentest em 2 modelos distintos de execução e em 2 modelos distintos de contratação: (a) ou como serviço contínuo (Preço global por projeto), tendo como escopo todos os ativos de TIC do órgão, ou como serviço com escopo definido para um projeto (Unidade de Serviço Técnico), ativo ou instância bem definida. Destes dois modelos, o mais adequado para as necessidades do BCB é o primeiro (Preço global por projeto); e (b) ou como item individualizado de contratação ou como um dos vários subitens da contratação de um serviço de segurança. Destes dois modelos, o mais adequado para as necessidades do BCB é o segundo, pois há necessidade de mais de 1 tipo de serviço especializado de segurança da informação para além do Pentest.

O modelo escolhido busca se ater às melhores práticas em que individualiza e separa preços de tipos de serviço distintos no lugar de agrupá-los sob uma mesma rubrica e dificultar a sua diferenciação. Além disso, ao adotar o escopo de prestação de serviço continuado e não limitado a um conjunto seleto de soluções, busca-se obter economia de escala na contratação do serviço ao manter um relacionamento com a mesma prestadora de serviço por mais tempo, preservando o acúmulo de familiarização que a eventual contratada teria com os sistemas do Banco Central, então tendo potencial de aumento da produtividade do serviço com o passar dos anos.

8.1.4. SERVIÇO DE GESTÃO DE VULNERABILIDADES

Realizou-se a busca pelos termos “Gestão” e “Vulnerabilidades”, tendo então um retorno de 105 registros. Filtrando cada um dos resultados pelos termos “vulnerabilidades”, “licença”, obteve-se um retorno de 22 e 4 registros respectivamente a cada termo.

O Edital nº 90.253/2025 do órgão DNIT [28] trata de contratação de licença para solução de gestão de vulnerabilidades em ativos, um modelo não necessário para as atuais necessidades do BCB, dado que o ambiente já se encontra monitorado por soluções de inventário de ativos e monitoramento de exposição de vulnerabilidades. A mesma situação se repete para os editais nº 10/2023 (CGRL) [29], nº 90.048/2024 (TJBH) [30], nº 90.047/2025 (Prefeitura de Macaé) [31], nº 54/2023 (TJDFT) [32], nº 90.008/2025 (PC-DF) [33], nº 90.028/2024 (TCE-RJ) [34], nº 90.007/2024 (DETRAN-RO) [35], nº 90.068 /2025 (Banco do Nordeste) [36], nº 30/2025 (SEFAZ-SC) [37], nº PERP20/2025 (Governo do RJ) [38], nº 90.025/2025 (MPU) [39], nº 90.038/2025 (Butantã) [40], nº 90.005/2024 (PRODEPA) [41].

Alguns casos desviam do escopo pretendido esta contratação, sendo então simplesmente descartados, como os editais de nº 90.086/2025 (TJRO) [42], que se trata de uma contratação de serviço de SOC.

O Edital de nº 60/2023 (TSE) [43] acumula a contratação de solução de um licenciamento para detectar vulnerabilidades em ativos e em imagens de containers. Da mesma forma, o edital de nº 194 /2024 (TCE-MG) [44] também contrata licença para detecção de vulnerabilidades em ativos e em imagens de containers no mesmo item de compra.

Dentre os editais que tratam de venda de serviço de gestão de vulnerabilidades nos termos demandados nesta contratação, há o edital nº 90.088/2025 (TJSP). Entretanto, este edital embute em um único item de compra a agregação de outros serviços que não são de interesse desta contratação como o serviço de administração, operação e manutenção e atendimento a requisições, o serviço de gestão de incidentes de segurança e serviço de monitoramento e visibilidade de ataques cibernéticos. Por outro lado, agrega, para além do item de serviço de gestão de vulnerabilidades, o serviço de testes de invasão. Esta contratação estipulou um prazo de 5 anos de duração e apresentou um valor total de R$ 55.850.702,70.

Outro edital similar é o nº 90.018/2024 (EPE) [45] como serviço de gerenciamento de vulnerabilidades, mas deixa para a contratada a responsabilidade de instalar e utilizar uma ferramenta de inventário e detecção no ambiente do órgão. O valor do contrato para 3 anos de vigência foi de R$ 1.162.635,82.

Em síntese, as diferentes formas de contratação de soluções de gerenciamento de vulnerabilidades realizadas por outros órgãos públicos têm se concentrado na aquisição de licenças de ferramentas de inventário de ativos e monitoramento de exposição a vulnerabilidades. Como o BCB já possui soluções para atender a este requisito, tais contratações são desconsideradas quanto a modelo de fornecimento. Em contraste, há alguns órgãos públicos que adotaram um modelo similar de contratar o gerenciamento de vulnerabilidades como serviço, agregado a uma licença a ser gerenciada pela contratada (Preço global por projeto). Deste modelo, o único componente de interesse ao BCB é o de fornecimento do serviço não acompanhado de aquisição de licença, o que pode fazer do modelo visado pelo BCB ser mais barato do que estes modelos em comparação.

8.1.5. LIÇÕES APRENDIDAS

As contratações analisadas evidenciam que (1) a agregação de licenças de ferramentas com serviços dificulta a segregação de preços e a avaliação de economicidade específica por componente; (2) modelos de pentest por escopo único reduz a continuidade e curva de aprendizado do fornecedor, elevando custo transacional; (3) quando há serviço contínuo e segregação de preços por tipo de serviço, há maior transparência, previsibilidade e potencial de ganho de escala ao longo do contrato; (4) a maioria das empresas pesquisadas são capazes de oferecer todos os 4 (quatro) serviços que endereçam as necessidades apresentadas, então existindo a possibilidade de uma única empresa oferecer todos os itens simultaneamente. Estes pontos orientam a opção do BCB por segregar licenças de quaisquer serviços e por priorizar prestação de serviço contínua nos itens aplicáveis.

Além disso, a ausência de contratações similares para inspeção manual de código e modelagem de ameaças /avaliação preventiva de riscos decorre, em hipótese, da diferença de demanda por revisões de segurança para a implantação de novas soluções nos respectivos ambientes de cada órgão. Com a vazão demandada para o BCB e buscando atender aos objetivos estratégicos institucionais de oferecer resiliência ao sistema financeiro nacional com uma segurança cibernética robusta, justifica-se a necessidade de contratação atípica pelo BCB.

Sintetizando o resultado da pesquisa por comparação de contratações similares no setor público, apresenta-se a tabela a seguir:

Serviço	Editais pertinentes no PNCP	Similaridades com a demanda do BCB	Conclusão
Inspeção manual de código	0	Praticamente inexistente	Contratação é inédita e especializada

Modelagem de ameaças / Risco	0	Apenas pentests ad-hoc	Contratação é inédita e especializada
Pentest	8	3 similares	Modelo contínuo e integrado é mais adequado
Gestão de vulnerabilidades	13 de licenças de ativos; 2 de licenças de ativos e de containers; 2 de serviços.	BCB já possui ferramenta de GV de ativos. Demanda serviço.	Serviços de gestão são viáveis, mas licenças de ativos são desnecessárias.

8.2. **ALTERNATIVAS DE MERCADO**

Para realizar a pesquisa de alternativas de mercado, foi realizado, com motor de busca, uma pesquisa com os termos “serviço de”, acompanhado de termos relacionados às necessidades especificadas para esta contratação como “avaliação de riscos”, “testes de invasão”, “gestão de vulnerabilidades” e “revisão de código fonte”. Desta pesquisa, encontrou-se a página web de 34 empresas que se propunham a fornecer os serviços pesquisados. Dessas 34, apenas foi possível obter um canal de contato comercial de 26. Ao entrar em contato com estas empresas, 3 responderam não conseguir prestar todos os serviços desejados simultaneamente e 2 retornaram com uma proposta comercial indicando ser capaz de oferecer todos os 5 serviços.

Entretanto, apesar da falta de respostas para levantamento de alternativas do mercado, ao avaliar o catálogo de serviços apresentados em seus respectivos sítios eletrônicos (websites), foi possível aferir que há a previsão de fornecimento de todos os serviços que o BCB necessita, conforme explicado a seguir.

Para a necessidade de inspeção de segurança do código fonte, esta necessidade é contemplada como uma das abordagens da área de Segurança de Aplicações (Application Security, ou AppSec). Esta abordagem também é referida como testes caixa branca ou revisão de código fonte. Esta abordagem consiste no exame crítico da infraestrutura, arquitetura, codificação e projeto da solução sendo analisada. Das empresas encontradas, foi possível validar a existência de prestação de serviço de inspeção de código fonte manual, então se distinguindo de empresas que apenas forneciam venda de licenças de software de revisão automatizada de código fonte.

A contratação de licenças de software de revisão automatizada de código fonte não atende às necessidades desta contratação, devido às limitações levantadas da literatura científica e de boas

práticas para a atividade. A partir da pesquisa de opinião de analistas de segurança realizada pela OWASP [6], apurou-se que ferramentas automatizadas eram boas alternativas para detectar vulnerabilidades e atender requisitos de conformidade (compliance). Entretanto, destituídas da capacidade de análise contextual, conhecimento de domínio, interpretação de cadeias longas de fluxos de dados, o resultado da pesquisa apontou que a percepção de analistas para a análise de deficiências em código fonte que culminavam em problemas de disponibilidade, privacidade e regras de negócio, atividades manuais de pentest e inspeção de código fonte eram alternativas melhores do que o uso de ferramentas automatizadas de SAST.

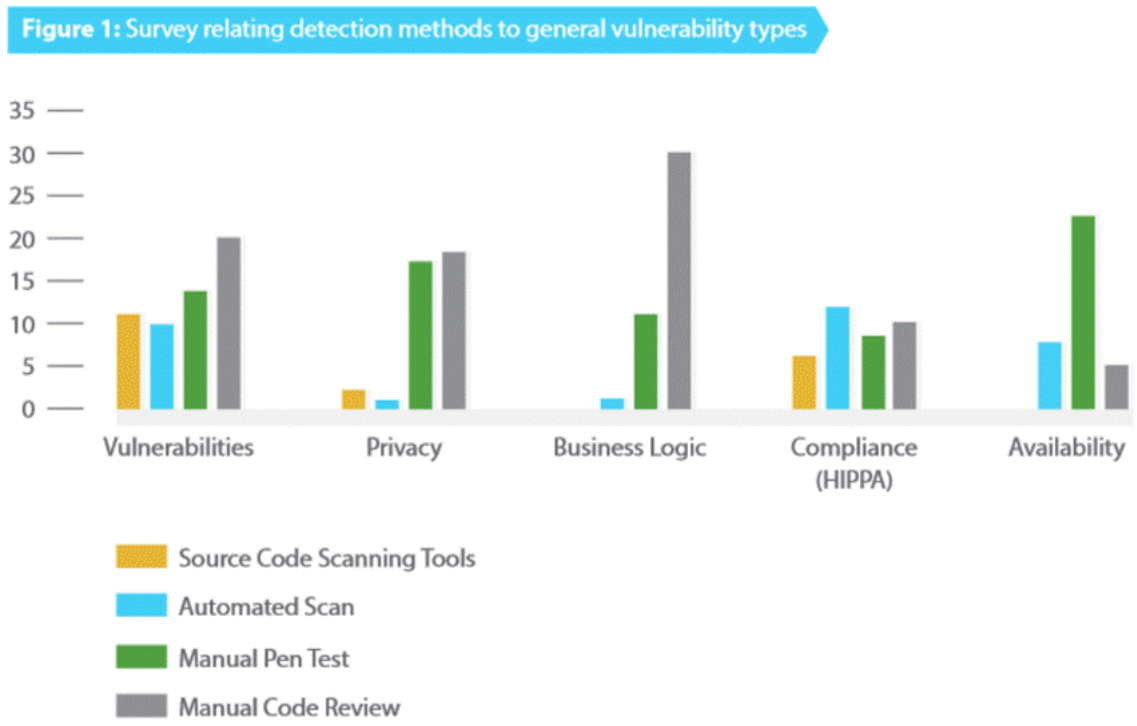


Figura 1: Resultado de pesquisa de opinião de analistas de segurança da informação quanto a qual o melhor método para detectar cada tipo de vulnerabilidade. A detecção de problemas em regras de negócio por meio de inspeção manual de código fonte foi considerada a melhor abordagem. Já em termos de vulnerabilidades conhecidas passam a ter uma melhor consideração de ferramentas de scan de código automatizado.

Em estudo dedicado sobre a comparação e avaliação de efetividade, consistência e performance de SAST automatizado na linguagem java [18], percebeu-se que tais ferramentas, apesar de apresentarem boa performance em repositórios sintéticos (artificialmente criados para servirem de benchmark para testar este tipo de ferramenta) tinham uma performance ruim para detectar vulnerabilidades em repositórios de código reais (eram capazes de detectar apenas 12,7% das vulnerabilidades que conheciam existir em meio ao código fonte). Mesmo combinando diferentes ferramentas simultaneamente, 70,9% das vulnerabilidades permaneciam indetectadas. Dessa forma, concluiu-se que a mera contratação de tais ferramentas não satisfazem as necessidades de revisão segura de código fonte do ambiente do BCB.

Baseado nestas informações, dos dois modelos de contratação levantados do mercado, concluiu-se que a prestação de serviço de inspeção manual de código fonte é o mais apropriado para endereçar as necessidades de revisão de segurança das soluções desenvolvidas pelo BCB. O resultado da pesquisa apurou que empresas como Ostec [46], Vantico [47], LoPrestiSec [48], Skyone [49] e

Tempest [50] ofereceriam o serviço de inspeção de código-fonte, havendo então disponibilidade de oferta suficiente no mercado para este serviço, apesar de não terem sido encontradas contratações similares por outros órgãos públicos para o serviço.

Ao pesquisar alternativas de prestação de serviço de apoio a processos de avaliação de riscos e de modelagem de ameaças, encontrou-se uma variedade de empresas fornecendo o serviço dentro da categoria de “Serviços de Governança Risco e Compliance”. O que foi possível verificar é não ter um nome padronizado para o serviço desejado, mas uma variedade de termos que redundam na necessidade especificada para o BCB. Algumas empresas oferecem o serviço sob o nome de “Gestão de riscos de segurança”, outras sob o nome de “Modelagem de ameaças”. Exemplificando a variedade de empresas contratadas alegando oferecer esse serviço constam a LoPrestiSec, Vantico, Ostec, Tempest e a Skyone. Baseado nesta amostragem, identificou-se que há disponibilidade de oferta suficiente no mercado para este serviço, apesar de não terem sido encontradas contratações similares por outros órgãos públicos.

Para a prestação de serviços de gestão de vulnerabilidades e de pentest, há uma grande variedade de empresas capazes de ofertar o serviço no modelo de escopo específico e de teste continuado. Este entendimento de disponibilidade persiste da última pesquisa realizada para o provimento do último contrato de serviço similar realizado pelo BCB, que será substituído por esta nova contratação. Consultando o catálogo disponibilizado nos portais web dessas empresas, foi possível identificar uma variedade de empresas que ofereciam tais serviços como a Tempest, LoPrestiSec, Enygma [52], Vantico, Clavis [51], Dia Zero Security [53], Ostec, Secure Tecnologia [54], dentre outras. Baseado nesta amostragem, identificou-se que há disponibilidade de oferta suficiente no mercado para este serviço.

8.3. EXISTÊNCIA DE SOFTWARE PÚBLICO BRASILEIRO

O portal do Software Público Brasileiro foi consultado para verificar a existência de algum software público disponível que atendesse às necessidades deste contrato, conforme especificado pela norma STI/MP nº 46 [55]. Foram pesquisados os termos no dia 15 de janeiro de 2026 às 10h16:

- invasão;
- pentest;
- vulnerabilidade;
- código;
- risco

A pesquisa apenas retornou um software: Ágatha - Sistema de Gestão de Riscos e Integridade [56]. Ele não será considerado, pois em sua descrição consta que "O sistema deixou de ser uma solução compartilhável como Software Público" e não recebe atualização desde 7 de maio de 2018. Cabe também enfatizar que a necessidade de contratação é por um serviço de apoio às atividades de modelagem de risco e que dificilmente seria atendido por um software de apoio.

Dessa forma, não há alternativas disponibilizadas no portal de software público brasileiro que atendam aos requisitos e necessidades do presente certame.

8.4. NECESSIDADE DE ADEQUAÇÃO A PADRÕES DE GOVERNO

As soluções que são objeto deste processo de contratação não buscam se integrar como plataforma disponível ao público ou se integrar aos sistemas estruturantes da administração pública. Desta forma, não consta em seus requisitos não-funcionais a sua adequação a padrões de governo como o ePing, eMag, ePwg, Design System do governo, ICP-Brasil, ou ao e-ARQ.

8.5. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO BCB

Não há necessidades de adequação do ambiente do BCB para receber a prestação de serviço, uma vez que, na sua especificação técnica, é esperado que o serviço se adeque aos processos já definidos pelo BCB.

8.6. DIFERENTES MÉTRICAS DE PRESTAÇÃO DE SERVIÇO PARA PAGAMENTO

Com os editais avaliados, foi possível encontrar, para gerenciamento de ativos e vulnerabilidades, os editais nº 90.088/2025 (TJSP) e o nº 90.018/2024 (EPE).

O edital da EPE utiliza 3 (três) indicadores de NMS (Nível Mínimo de Serviço, a métrica de SLA para fiscalização do contrato): (1) tempo máximo para requisição de mudança para aplicação de patches e hotfixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente, com meta estipulada de atendimento em no máximo 72 horas, com o eventual descumprimento sujeito à glosa de 1% do valor da parcela mensal. (2) prazo de entrega de relatórios de avaliação de vulnerabilidades e sugestões de correções, com meta estipulada de 10 dias úteis, com o seu descumprimento sujeito à glosa de 0,5% do valor mensal do contrato. (3) Entrega de 9 relatórios de análises de vulnerabilidades, havendo margem de tolerância para entregar até no mínimo 7 relatórios por mês, sujeito a 0,5% de glosa do valor mensal do contrato em caso de descumprimento.

Por outro lado, o edital do TJSP cria um sistema que atribui pontos para cada ocorrência de desvio do fornecimento aos requisitos de entrega. A cada ponto, seria aplicada uma glosa de 0,1% sobre o valor da parcela mensal. Além disso, também aplica glosa de 0,1% para cada ponto de desvio dos KPIs definidos de entrega em relação às metas definidas em termo de referência, que seriam métricas relativas a índices de interação com clientes.

Comparando os dois modelos de fiscalização, é possível notar que a contratação da TJSP é mais rigorosa e metódica em termos de fiscalização que a contratação da EPE. Entretanto, cabe perceber que ambos os modelos de fiscalização utilizam como métricas de glosa parâmetros de disponibilidade da entrega, mas não há critérios de medição de qualidade da entrega. O parâmetro de glosa que mais se aproxima a um parâmetro orientado à qualidade da entrega é apresentado pelo TJSP com métricas orientadas à avaliação de clientes atendidos por chamados. Cabe, no entanto, frisar que este modelo de avaliação está centrado em avaliações subjetivas do cliente avaliador e não em avaliações objetivas, capazes de medir aspectos técnicos da entrega da contratada.

Dessa forma, 4 (quatro) lições foram aprendidas a partir da comparação de métodos de fiscalização de contrato:

- O objeto central da avaliação de um serviço de gestão de vulnerabilidades é o relatório /notificação de correção/avaliação de vulnerabilidades. É com base neste artefato que é possível medir prazos de entrega, número de entregas e a sua qualidade, ao avaliar o seu conteúdo.

- Para avaliar um serviço de gestão de vulnerabilidades, é importante medir o tempo de resposta medido entre a tomada de conhecimento de uma vulnerabilidade relevante de ser corrigida e o envio de sua notificação para correção à área interessada;
- Para avaliar um serviço de gestão de vulnerabilidades, é importante medir a quantidade de relatórios/notificações de correções de vulnerabilidades entregues às áreas interessadas;
- É preciso estipular critérios objetivos para avaliar a qualidade da entrega de um serviço de gestão de vulnerabilidades, com base em características intrínsecas do relatório/notificação de correção /avaliação de vulnerabilidades em detrimento de atribuições extrínsecas e subjetivas do demandante da análise.

Já para os serviços de Pentest para serviço contínuo, foi possível encontrar os editais nº 90.078/2025 (CODEVASF), nº 90.007(5)/2025 (FMABC) e nº 90.088 (TJSP).

O modelo de fiscalização do TJSP aplicado para o serviço de pentest é similar ao modelo de fiscalização para gestão de vulnerabilidades. Dessa forma, o método se limita a avaliar a disponibilidade, respeito a prazos e não ter intercorrências durante a prestação do serviço. O edital da FMABC não apresentou descrições suficientes e detalhadas sobre critérios de fiscalização de serviço de pentest, se limitando apenas a estipular prazos para a entrega de relatórios de análise. O edital da CODEVASF apresenta um modelo mais enxuto de avaliação do serviço baseado em 2 (duas) métricas: (1) cobertura de escopo do pentest, que consiste em uma razão entre o número de ativos testados e o número de ativos no plano de execução; (2) prazos de entrega.

Comparando os 3 (três) modelos de fiscalização, é possível perceber que prazos de entrega do pentest e escopo tem sido os principais elementos avaliados. Diferentemente do modelo a ser adotado no BCB, os pentests têm admitido como escopo a totalidade da infraestrutura dos órgãos. Para a necessidade do BCB, o escopo de cada análise se limitaria a analisar dois sistemas a cada mês. Dessa forma, seria possível granularizar os critérios de fiscalização de execução do contrato para cada análise de sistema.

Dessa forma, 3 (três) lições foram aprendidas a partir da comparação de métodos de fiscalização de contrato:

- O objeto central da avaliação de um serviço de pentest é o relatório final. É com base neste artefato que é possível medir prazos de entrega e a sua qualidade, ao avaliar o seu conteúdo.
- É preciso estipular critérios objetivos para avaliar a qualidade da entrega de um serviço de pentest, com base em características intrínsecas do relatório em detrimento de atribuições extrínsecas e subjetivas do demandante da análise.
- Uma métrica utilizada para avaliar a cobertura da execução do serviço, é preciso verificar a cobertura de número de ativos testados e a profundidade com o qual foram testados.

8.7. RESUMO DAS SOLUÇÕES LEVANTADAS

Após estudo de contratações similares e de pesquisas de mercado, foi possível levantar um conjunto de modelos de prestação de serviço, enumerados na tabela a seguir:

Id	Descrição da solução (ou cenário)
1	Contratação de serviços contínuos

2	Contratação de serviços por escopo específico
3	Não contratar serviço de apoio

9. Análise comparativa de soluções

Como auxílio, o quadro seguinte compara os 3 modelos de soluções identificadas. Os requisitos descritos na tabela a seguir estão relacionados às necessidades de negócio, tecnológicas e aos requisitos necessários e suficientes para escolha da solução de TIC descritos nas seções 4, 5 e 6 deste documento. As células dos cenários apresentados são preenchidas com valores A (Atende) e N (Não atende). Na última linha, é apresentado como resultado da análise um percentual de atendimento de requisitos por cada cenário.

Requisitos		Cenários		
		1	2	3
Negócio	Ter a capacidade de, com precisão, monitorar a exposição de ativos de TIC inventariados do BCB a novas vulnerabilidades descobertas	A	A	A
	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	A	A	A
	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	A	N	N
	Ter a capacidade de, continuamente, testar a efetividade das funcionalidades de segurança conforme codificado nas soluções internas do BCB	A	N	N
	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	A	A	A

	Realizar o monitoramento contínuo de vulnerabilidades relacionadas aos softwares, componentes e serviços utilizados nos ambientes do BCB.	A	A	A
	Classificar e contextualizar vulnerabilidades com base no impacto específico ao ambiente institucional, indo além de métricas genéricas como CVSS.	A	A	A
	Permitir comunicação técnica precisa com as equipes responsáveis pela manutenção dos sistemas, incluindo descrição da vulnerabilidade, impacto, e recomendações de correção.	A	A	A
	Manter processos e interfaces seguras para inventário e gestão de exposição de ativos.	A	N	A
	Oferecer mecanismos de alerta tempestivos, com priorização automática baseada em critérios de severidade técnica e risco operacional.	A	A	A
	Disponibilizar capacidade de realização de testes de invasão sob demanda, abrangendo aplicações, serviços e infraestruturas.	A	A	A
	Execução de técnicas representativas de atacantes reais, incluindo vetores externos e internos, com cobertura de táticas e técnicas relevantes.	A	A	A
	Capacidade de adaptação de profundidade dos testes conforme complexidade e criticidade dos sistemas avaliados.	A	A	A
	Relatórios técnicos completos, contendo evidências, impacto, risco e recomendações de correção.	A	A	A
Tecnológicos	Execução escalável, permitindo atender variações na demanda institucional sem afetar prazos de entrega operacional.	A	N	N
	Prover serviço de análise manual especializada de segurança de código abrangendo vulnerabilidades de implementação, lógica de negócio e arquitetura.	A	A	A

	Capacidade de identificar fluxos de dados, dependências e comportamentos complexos, que não são detectados por análises automatizadas.	A	A	A
	Avaliação segura de múltiplas linguagens e frameworks, conforme adotado nos sistemas do BCB, priorizando Java-Spring, C#-.Net, Node.JS-angular e Python.	A	A	A
	Emissão de relatório detalhado, contendo diagnósticos, classificação, exploração possível, impacto e recomendações.	A	A	A
	Realizar modelagem estruturada de ameaças para sistemas internos e de terceiros, incluindo soluções em nuvem.	A	A	A
	Identificar cenários de risco, atores de ameaça e vulnerabilidades estruturais, considerando aspectos técnicos e funcionais.	A	A	A
	Fornecer estimativas de risco cibernético com base na metodologia CIS-RAM v2.2.	A	A	A
	Recomendar controles mitigatórios adequados ao risco e ao ambiente do BCB.	A	A	A
	Apoiar avaliações extraordinárias conforme surgimento de novas soluções ou alterações arquiteturais relevantes.	A	A	A
Outros	Os profissionais responsáveis por prestar o serviço solicitado deverá ter experiência comprovada de 5 (cinco) anos, ao longo dos últimos 6 (seis) anos, em Segurança da informação, possuindo Pós-graduação em segurança da informação ou em TI.	A	A	A
	Os profissionais devem ter certificações profissionais, conforme as enumeradas anteriormente.	A	A	A
	Os serviços devem ser oferecidos por uma equipe integrada com possibilidade de diálogo e intercâmbio de informações, pois os insumos gerados por um processo serão utilizados em outro (e.g.: Os modelos de ameaça gerados pelo serviço de modelagem de	A	N	A

	ameaças e avaliação de riscos podem ser usados como documentação para os processos de pentest e revisão de código fonte).			
Resultado da análise		100%	82%	89%

O cenário 2, referente à contratação de serviços não continuados e delimitados por escopo, não atende a 5 requisitos, sendo eles 2 de negócios, 2 tecnológicos e 1 de outro tipo. Já o cenário 3, que consiste em esforço interno de servidores para atender à demanda, não atende a 3 requisitos, sendo 2 de negócios e 1 tecnológico. A seguir, é apresentada uma listagem justificando o motivo do não atendimento de cada um destes requisitos pelo modelo de contratação:

- 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.
    - O modelo de contratação por escopo específico não é adequado para escalar, redimensionar e redirecionar esforços e recursos em resposta a variações imprevisíveis na demanda institucional da instituição. Como a carga de análises é variável, é difícil de delimitar um escopo preliminar a ser firmado em contrato. Além disso, sendo a estrutura de TI do BCB de grandes dimensões e diversa, ao delimitar um escopo vago e amplo como um que especifique todos os sistemas de TI do banco terminaria por coincidir, mas de forma menos estruturada, com o modelo de contratação de prestação de serviço contínuo.
    - Para o cenário de atendimento por esforço interno, não há capacidade de prover o requisito de forma contínua, dado que com o quadro reduzido de funcionários, não existe a possibilidade de 2 servidores abdicarem de suas atribuições para se dedicarem à tarefa de teste de invasão.
- Ter a capacidade de, continuamente, testar a efetividade das funcionalidades de segurança conforme codificado nas soluções internas do BCB.
    - O modelo de contratação por escopo específico não é adequado por não haver garantia de continuidade e acúmulo de entendimento de padrões de projeto e código, vocabulário de domínio e paradigmas de arquitetura utilizados pelo BCB entre as análises. Dessa forma, compromete-se os ganhos de eficiência das análises de código fonte que poderiam ser adquiridos com o acúmulo de experiência por um profissional dedicado. Além disso, isso comprometeria eventual economia de escala ao custear, reiteradas vezes, o custo de tempo de familiarização de novos profissionais com cada projeto e a arquitetura de projeto do BCB.
    - Para o cenário de atendimento por esforço interno, não há capacidade de prover o requisito de forma contínua, dado que com o quadro reduzido de funcionários, não existe a possibilidade de 1 servidor abdicar de suas atribuições para se dedicar à tarefa de inspeção manual de código fonte.
- Manter processos e interfaces seguras para inventário e gestão de exposição de ativos.
    - Um processo de gestão de vulnerabilidades não pode ser provisionado por escopos delimitado como um projeto, uma vez que se trata de um acompanhamento, ao longo do

tempo, da integridade de ativos frente a vulnerabilidades. A correção de um conjunto de vulnerabilidades presentes em um sistema em um momento não garante a sua não exposição a novas vulnerabilidades publicadas em um momento futuro.

- Execução escalável, permitindo atender variações na demanda institucional sem afetar prazos de entrega operacional.
    - O modelo de contratação por escopo específico não é adequado para escalar, redimensionar e redirecionar esforços e recursos em resposta a variações imprevisíveis na demanda institucional da instituição. Como a carga de análises é variável, é difícil de delimitar um escopo preliminar a ser firmado em contrato. Além disso, sendo a estrutura de TI do BCB de grandes dimensões e diversa, ao delimitar um escopo vago e amplo como um que especifique todos os sistemas de TI do banco terminaria por coincidir, mas de forma menos estruturada, com o modelo de contratação de prestação de serviço contínuo.
    - Para o cenário de atendimento por esforço interno, não há capacidade de prover o requisito de forma escalável, dado que com o quadro reduzido de funcionários, há rigidez na disponibilidade de oferta de tarefas de teste de invasão.
- Os serviços devem ser oferecidos por uma equipe integrada com possibilidade de diálogo e intercâmbio de informações, pois os insumos gerados por um processo serão utilizados em outro (e.g.: Os modelos de ameaça gerados pelo serviço de modelagem de ameaças e mensuração de riscos podem ser usados como documentação para os processos de pentest e inspeção de código fonte).
    - O modelo de contratação por escopo específico limitaria a integração e sinergia esperadas para garantir a qualidade das entregas de cada processo para apenas o escopo do sistema delimitado na contratação. Pela arquitetura dos sistemas do BCB serem integrados com diversos sistemas, é importante que o conhecimento de avaliação de segurança de um sistema se preserve ao avaliar outro sistema com o qual ele interage.

O atendimento com ressalvas para o cenário em que não se contrata os serviços se justifica pelo fato dos servidores do BCB serem tecnicamente capazes de realizar os processos detalhados. Entretanto, este atendimento enfrenta restrições de recursos humanos e tempo, dado o número de servidores ativos, o que implicaria na degradação ou não atendimento de outras atribuições funcionais destes servidores ao deixarem de operar outros processos não cobertos nesta contratação para ser possível atender aos requisitos de regularidade, tempestividade e profundidade esperados para estes processos.

10. Registro de soluções consideradas inviáveis

Desta forma, o cenário 2, referente à contratação de serviços não continuados e delimitados por escopo, foi considerado inviável como modelo de prestação de serviço deste projeto, então sendo não considerado para a análise comparativa de custo total de propriedade (TCO). Além disso, o cenário 3 também foi considerado inviável, dado que a restrição de recursos humanos se demonstrou um fator que degrada ou não atende os requisitos devido ao fato de não haver margem de redistribuição de atribuições funcionais de servidores de forma a preservar as outras atribuições funcionais estratégicas, então não sendo possível atender os requisitos de regularidade, tempestividade e profundidade esperados para estes processos.

Além de apontar a limitação de atendimento do esforço interno, é importante mencionar os apontamentos de normas técnicas de segurança da informação sugerindo que testes e avaliações de segurança realizados de forma independente sejam desejáveis, então indicando ser mais interessante seguir pela alternativa de serviço contínuo terceirizado, conforme enumerado a seguir:

- CIS Controls, controle 18 de Testes de invasão: “Os testes de invasão independentes podem fornecer percepções valiosas e objetivas sobre a existência de vulnerabilidades [...]” [57]
- NIST SP 800-53, revisão 5, Capítulo 3.4 sobre avaliações, autorizações e monitoramento, em seu controle sugerido CA-2, que trata de avaliações de controles, fala sobre os benefícios de avaliações de segurança contarem com a avaliação de avaliadores independentes, desde que o seu trabalho não apresente conflito de interesses que possa conflitar com a qualidade e imparcialidade da avaliação. [58]
- ISO 27001, Anexo A, controle 5.35 recomenda que revisões de segurança da informação sejam realizadas de forma independente de forma periódica ou quando mudanças relevantes ocorrerem. [59]

Assim, concluiu-se que apenas uma das alternativas se demonstrou como viável para atender aos requisitos levantados por esta contratação.

11. Análise comparativa de custos (TCO)

Apesar de não haver uma alternativa para se realizar a comparação de custo total de propriedade, apresenta-se os cálculos de custos levantados para a alternativa remanescente de contratação de serviços contínuos especializados de segurança da informação.

Conforme detalhado na seção de pesquisa de necessidades similares na administração pública, verificou-se a inexistência de contratações por alguns serviços como o de inspeção manual de código fonte e de mensuração de riscos cibernéticos. Tal ausência de referências tornou-se um empecilho para estimar um custo de contratação para este projeto.

Uma nova pesquisa de contratos no PNCP foi realizada na data de 24/04/2026, então considerando contratos vigentes ou cuja data de vigência tenha expirado há no máximo 1 (um) ano (24/04/2025). Com isso, foi possível obter a listagem de contratações no serviço público para os serviços relacionados a testes de invasão e a gestão de vulnerabilidades nas Tabela 1 e Tabela 2. O valor de cada contratação foi adaptado para o mesmo prazo de vigência da necessidade deste projeto de 48 meses para fins de comparação. Além disso, alguns contratos que acumulavam os serviços de Pentest e GAV sob a mesma rubrica passaram por um processo de decomposição de valores, com metodologia detalhada nas Tabela 3 e Tabela 4.

Tabela 1: Contratos similares obtidos do PNCP vigentes ou encerrados há no máximo 1 ano para serviços de teste de invasão (pentest). A última coluna ajusta os valores para a mesma base comum de comparação de prazo para o projeto do presente ETP.

Edital	Valor	Prazo (Meses)	Valor por mês	Valor total em 48 meses

90005/2025 [61]	R$	128.498,40	12	R$	10.708,20	R$	513.993,60
90007/2025 [62]	R$	128.498,40	12	R$	10.708,20	R$	513.993,60
90023/2025 [63]	R$	202.657,98	12	R$	16.888,17	R$	810.631,92
247/2025/2025 [64]	R$	12.812,50	4	R$	3.203,13	R$	153.750,00
90024/2025 [65]	R$	1.333.280,00	60	R$	22.221,33	R$	1.066.624,00
90078/2025 [66]	R$	120.000,00	24	R$	5.000,00	R$	240.000,00
90054/2024 [67]	R$	31.171,67	0,5	R$	62.343,34	R$	2.992.480,32
90088/2025 [68]	R$	6.505.542,29	60	R$	108.425,70	R$	5.204.433,83
90048/2024 [69]	R$	641.660,00	24	R$	26.735,83	R$	1.283.320,00

Tabela 2 Contratos similares obtidos do PNCP vigentes ou encerrados há no máximo 1 ano para serviços de gerenciamento de ativos e vulnerabilidades. A última coluna ajusta os valores para a mesma base comum de comparação de prazo para o projeto do presente ETP.

Edital	Valor		Prazo (Meses)	Valor por mês		Valor total em 48 meses	
247/2025/2025 [64]	R$	43.562,50	4	R$	10.890,63	R$	522.750,00
90088/2025 [68]	R$	6.505.542,29	60	R$	108.425,70	R$	5.204.433,83
90009/2025 [70]	R$	662.083,32	12	R$	55.173,61	R$	2.648.333,28
90048/2024 [69]	R$	5.330.550,72	24	R$	222.106,28	R$	10.661.101,44

Tabela 3 Memória de cálculo da decomposição dos subitens constituintes do contrato relativo ao edital de número 247/2025/2025

Distribuição do valor do contrato de edital 247/2025 por grupo de serviço em função do número de perfis profissionais				
Nº do Edital	247/2025/2025	Valor global (VG)	R$ 56.375,00	
Subitem	**Tipo**	**Horas**	**Custo Relativo (CR)**	**CR x VG**
Mapeamento e inventário de aplicações	GAV	40	9%	R$ 5.125,00
Atividades técnicas de avaliação de vulnerabilidades	GAV	300	68%	R$ 38.437,50
Teste de penetração (Pentest)	Pentest	100	23%	R$ 12.812,50
Total		440		

Total do valor de cada tipo de serviço somando os subitens do contrato avaliado	
Tipo	**Valor total**
GAV	R$ 43.562,50
Pentest	R$ 12.812,50

Tabela 4 Memória de cálculo de decomposição dos valores dos subitens contidos no contrato relativo ao edital de número 90088/2025

Distribuição do valor do contrato de edital 90088/2025 por grupo de serviço em função do número de perfis profissionais					
Nº do Edital	90088/2025	Valor global (VG)	R$ 55.850.702,70		

Grupo de serviço	Nº de Jr	Nº de Pl	Custo estimado	Custo relativo (CR)	CR x VG
GAV	0	2	R$ 38.672,35	11,65%	R$ 6.505.542,29
Blue	0	4	R$ 77.344,69	23,30%	R$ 13.011.084,57
Pentest	0	2	R$ 38.672,35	11,65%	R$ 6.505.542,29
Monitoramento	2	0	R$ 28.563,35	8,60%	R$ 4.804.985,42
Infra	5	4	R$ 148.753,06	44,80%	R$ 25.023.548,13
Total			R$ 332.005,79		

Perfis profissionais da SGD/MGI nº 1.070/2023			
Perfil	Salário	Fator-K	Custo unitário
ASEG-01 (Jr)	R$ 6.966,67	2,05	R$ 14.281,67
ASEG-02 (Pl)	R$ 9.716,67	1,99	R$ 19.336,17

O consolidado da pesquisa é apresentado na Tabela 5. Então, aplicou-se a metodologia de cálculo de outlier por meio do critério de análise de quartis. Com isso, valores de contratos similares de gestão de vulnerabilidades e de testes de invasão que excederam os limites superiores e inferiores calculados foram descartados da amostra.

Tabela 5 Consolidado da pesquisa de preços pelo parâmetro de contratos similares da administração pública.

Tipo	Pentest	GAV
Média	R$ 2.355.343,61	R$ 4.223.912,91
Mediana	R$ 1.621.263,84	R$ 2.625.275,10
Menor	R$ 480.000,00	R$ 984.000,00

Desvio	R$ 1.941.139,64	R$ 4.360.687,29
CV	82%	103%
1º Q	R$ 1.027.987,20	R$ 2.197.662,69
3º Q	R$ 2.566.640,00	R$ 4.651.525,32
Amplitude IQ	R$ 1.538.652,80	R$ 2.453.862,63
Lim. Superior	R$ 4.874.619,20	R$ 8.332.319,27
Lim. Inferior	R$ 258.660,80	R$ 970.731,37

Dessa forma, foram descartados os preços de contratos de pentest 90054/2024 e 90088/2025 e o contrato de GAV 90048/2024. Além disso, foi depurado o número de profissionais empregados e a vigência em cada contrato para normalizar o preço para trazer à mesma base de comparação deste termo de referência. Com isso, a nova amostra de contratos similares sendo considerados para compor este parâmetro de pesquisa de preço é apresentado nas tabelas Tabela 6 e Tabela 7.

Tabela 6 Contratos similares obtidos do PNCP vigentes ou encerrados há no máximo 1 ano para serviços de teste de invasão (pentest) após descarte de contratos que apresentaram preço considerados outliers em análise de distância interquartil da amostra. Além disso, os valores são ajustados pelo número de funcionários empregados para se ajustar ao volume de serviço estimado para este termo de referência, então adaptando os valores para a mesma base de comparação.

Edital	Valor	Prazo (Meses)	Prestadores	Valor por mês	Valor 48 meses 2 profs	Órgão
90005 /2025	R$ 128.498,40	12	1	R$ 10.708,20	R$ 1.027.987,20	FMABC
90007 /2025	R$ 128.498,40	12	1	R$ 10.708,20	R$ 1.027.987,20	FMABC
90023 /2025	R$ 202.657,98	12	1	R$ 16.888,17	R$ 1.621.263,84	TJMSP
247/2025 /2025	R$ 12.812,50	0,625	1	R$ 20.500,00	R$ 1.968.000,00	Prefeitura de Taubaté

90024 /2025	R$ 823.012,35	60	1	R$ 13.716,87	R$ 1.316.819,75	CFM
90078 /2025	R$ 120.000,00	24	1	R$ 5.000,00	R$ 480.000,00	CODEVASF
90048 /2024	R$ 641.660,00	24	1	R$ 26.735,83	R$ 2.566.640,00	TJBA

Tabela 7 Contratos similares obtidos do PNCP vigentes ou encerrados há no máximo 1 ano para serviços de gestão de ameaças e vulnerabilidades após descarte de contratos que apresentaram preço considerados outliers em análise de distância interquartil da amostra. Além disso, os valores são ajustados pelo número de funcionários empregados para se ajustar ao volume de serviço estimado para este termo de referência, então adaptando os valores para a mesma base de comparação.

Edital	Valor	Prazo (Meses)	Prestadores	Valor por mês	Valor 48 meses 1 profs	Órgão
247 /2025 /2025	R$ 43.562,50	2,125	1	R$ 20.500,00	R$ 984.000,00	Prefeitura de Taubaté
90088 /2025	R$ 6.505.542,28	60	2	R$ 108.425,70	R$ 2.602.216,91	TJSP
90009 /2025	R$ 662.083,32	12	1	R$ 55.173,61	R$ 2.648.333,28	CODEMAR

Como resultado, o cálculo de estimativa de preço com base nesses valores foi consolidado na Tabela 8 . Ao realizar o cálculo de coeficiente de variação, como obteve-se um valor acima de 25% para ambas as amostras de contratos de Pentest e de GAV, foi considerado o valor de mediana para representar o resultado da pesquisa de preço pelo parâmetro de contratos similares pela administração pública.

Tabela 8 Consolidado da pesquisa de preços pelo parâmetro de contratos similares da administração pública após descartar itens de valores considerados outlier e adaptando os preços ao número de funcionários empregados para o mesmo quantitativo estimado para este termo de referência.

Tipo	Pentest	GAV
Média	R$ 1.429.814,00	R$ 2.078.183,40
Mediana	R$ 1.316.819,75	R$ 2.602.216,91

Menor	R$ 480.000,00	R$ 984.000,00
Desvio	R$ 689.989,67	R$ 947.871,12
CV	48%	46%

Para complementar a pesquisa de preço, também foi utilizado como parâmetro complementar o mapa de pesquisa salarial de referência para serviços de operação de infraestrutura e atendimento ao usuário publicado pela Portaria SGD/MGI nº 1.070/2023 em seu anexo II, de acordo com o Artigo 23 do parágrafo 1º, inciso III, por ser uma tabela de referência formalmente aprovada pelo Poder Executivo Federal. Foi adotado como perfil profissional de referência para a prestação do serviço o Administrador em segurança da informação – Sênior, o perfil ASEG-03. Além disso, foi feito um ajuste no custo de banco de horas por ser equivalente ao serviço de pentest contínuo, mas ajustado pela proporção de quanto que as horas contratadas anualmente representam de horas úteis de um ano, então representando um valor de 50%. Este cálculo de preço por subitem de serviço é apresentado na memória de cálculo da Tabela 9.

Tabela 9 Memória de cálculo para estimativa de preço de contratação de serviços de segurança da informação com base em pesquisa de salários por perfil profissional publicado pelo Anexo II da SGD /MGI nº 1.070/2023.

Estimativa de custo de contratação com base no custo de perfil profissional pelo mapa de pesquisa salaria de referência para serviços de TIC do Anexo II da SGD/MGI nº 1.070/2023 art. 2º			
Perfil profissional de referência	ASEG-03	**(A) Salário estimado**	R$ 15.056,97
(C) Duração do contrato em meses	48	**(B) Fator-K**	1,95
(D) Custo mensal estimado de profissional (A x B)	R$ 29.361,09	**(E) Custo total estimado por profissional (D X C)**	R$ 1.409.332,39
Subitem	**Descrição**	**(F) Quantidade de profissionais estimada**	**(G) Valor total (E x F)**

1	Serviço contínuo de gestão de vulnerabilidades (meses)	1	R$	1.409.332,39
2	Serviço contínuo de testes de invasão (pentesting) (meses)	2	R$	2.818.664,78
3	Serviço contínuo de inspeção de código fonte (meses)	1	R$	1.409.332,39
4	Banco de horas de testes de invasão (horas)	1	R$	704.666,20
5	Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (meses)	1	R$	1.409.332,39
Total (Soma de Gi)			R$	7.751.328,16

Ajustes no custo de banco de horas			
(A) Horas estimadas por dia	8	**(D) Dias úteis em um ano**	250
(B) Horas do banco de horas	4000	**(E) Dias de trabalho acionáveis (C/A)**	125
(C) Horas por ano (B / 4)	1000	**(F) Razão de uso do banco de horas no ano (E/D)**	50%

Para suprir as limitações desta pesquisa, o cálculo de estimativa foi complementado com o resultado do parâmetro de pesquisa direta com fornecedores no mercado. Com base na resposta de 4 empresas distintas, foi possível obter os valores estimados para os serviços especificados neste ETP. A seguir, são apresentadas as 4 propostas detalhando o preço anual de cada serviço solicitado. As propostas comerciais originais recebidas se encontram como anexo ao Processo Eletrônico associado a este ETP.

	Protiviti	**Clavis**	**Network Secure**	**Solo Network**

Gestão de vulnerabilidades	R$ 3.456.000,00	R$ 1.344.000,00	R$ 3.063.264,00	R$ 4.031.474,40
Pentest	R$ 6.912.000,00	R$ 3.360.000,00	R$ 3.407.328,00	R$ 7.256.653,92
Revisão de código	R$ 3.456.000,00	R$ 1.440.000,00	R$ 1.703.712,00	R$ 6.181.594,08
Banco de horas de pentest	R$ 1.800.000,00	R$ 1.400.000,00	R$ 888.000,00	R$ 2.687.649,60
Avaliação de risco	R$ 3.456.000,00	R$ 1.344.000,00	R$ 1.821.696,00	R$ 6.719.124,00
Preço global (4 anos)	R$ 19.080.000,00	R$ 8.888.000,00	R$ 10.884.000,00	R$ 26.876.496,00

Conforme orientação da IN ME nº 73/2020, exige-se a utilização da média como método de cálculo de estimativa de preço caso se trabalhe com uma amostra de dados homogênea e mediana em caso de dados heterogêneos e com menos observações. Em detalhamento fornecido pelo manual do STJ de orientação para pesquisa de preços, sugere-se que o critério de homogeneidade de valores seja medido com o cálculo de coeficiente de variação, calculado como a razão entre o desvio padrão e a média das amostras. Caso o coeficiente de variação seja menor que 25%, sugere-se adotar a média como método. Caso supere os 25%, sugere-se adotar a mediana. Com isso, calculou-se o coeficiente de variação das propostas de preço recebidas e inferiu-se que o método de cálculo indicado para esta estimativa é a mediana, conforme apresentado na memória de cálculo da Tabela 10.

Tabela 10 Consolidado das propostas de preços fornecidas por fornecedores em contexto de pesquisa direta.

Empresa	Preço Global
Protiviti	R$ 19.080.000,00
Clavis	R$ 8.888.000,00
Network Secure	R$ 10.884.000,00
Solo Network	R$ 26.876.496,00
Média	R$ 16.432.124,00

Mediana	**R$ 14.982.000,00**
Desvio Padrão	R$ 8.241.998,96
Coeficiente de Variação	50,16%

Combinando estes 3 parâmetros de pesquisa de preços: (1) contratos similares da administração pública; (2) estimativa com base em valor de salários de referência por perfil profissional a prestar o serviço; (3) propostas de preços obtidas diretamente com fornecedores, foi possível então realizar uma estimativa de preço a partir do cálculo de média com os valores obtidos de cada parâmetro, conforme apresentado na Tabela 11.

Tabela 11 Composição do valor de estimativa de preço da pesquisa de preço pela média da mediana dos contratos, mapa dos salários dos perfis profissionais a prestarem o serviço e a mediana das propostas obtidas a partir da pesquisa direta com fornecedores.

Subitem	Descrição	(A) Mediana de Contratos	(B) Mapa de salários	(C) Mediana das Propostas	Estimativa final (A + B + C / 3)
1	Serviço contínuo de gestão de vulnerabilidades (meses)	R$ 2.602.216,91	R$ 1.409.332,39	R$ 3.456.000,00	R$ 2.489.183,10
2	Serviço contínuo de testes de invasão (pentesting) (meses)	R$ 1.316.819,75	R$ 2.818.664,78	R$ 6.912.000,00	R$ 3.682.494,85
3	Serviço contínuo de inspeção de código fonte (meses)		R$ 1.409.332,39	R$ 3.456.000,00	R$ 2.432.666,20
4	Banco de horas de testes de invasão (horas)	R$ 658.409,88	R$ 704.666,20	R$ 1.800.000,00	R$ 1.054.358,69

5	Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (meses)		R$ 1.409.332,39	R$ 3.456.000,00	R$ 2.432.666,20
Total			**R$ 7.751.328,16**		R$ 12.091.369,03

Dessa forma, conclui-se que a estimativa de custo total de propriedade da contratação de serviços contínuos de segurança da informação especializados para 4 anos é de **R$ 12.091.369,03**.

12. Descrição da solução de TIC a ser contratada

A solução escolhida para atender às necessidades apresentadas neste estudo é a contratação de serviços contínuos especializados de segurança da informação de gestão de vulnerabilidades, testes de invasão - acompanhado de contratação de banco de horas para permitir a elasticidade da oferta de serviço para responder ao aumento na demanda de análises -, inspeção de código fonte e mensuração de riscos com um provisionamento estimado de 5 profissionais tecnicamente capacitados para um período de 4 anos, possivelmente prorrogável de acordo com o limite previsto na lei 14.133 [45].

Esta escolha fundamenta-se no reconhecimento do não atendimento do modelo de prestação de serviço limitado ao escopo orientado a sistemas. Dentre as deficiências de tal modelo, constam a incapacidade de oferecer a sinergia esperada na provisão de cada uma das verticais de serviço enumeradas, além de não oferecer economia de escala prevista com o acúmulo de experiência e entendimentos sobre os sistemas do BCB por não permitir uma continuidade temporal de prestação de serviço.

Além disso, este modelo de solução também é mais adequado do que endereçar as necessidades somente contando com o esforço interno de servidores, dado o quadro reduzido de servidores disponíveis.

Em conclusão, o modelo escolhido de solução é capaz de atender aos requisitos de negócio, técnicos esperados para o projeto apresentando um custo estimado condizente com o orçado.

A Tabela 12 discrimina os custos de cada item do serviço segundo a estimativa de preço resultante de forma anualizada, isto é, dividindo o valor de cada subitem por 4.

Tabela 12 TCO anualizado e discriminado por subitem do serviço.

Solução 1 - Contratação de serviços contínuos				
Ano ->	**2027**	**2028**	**2029**	**2030**
Item				

Serviços contínuos de Gerenciamento de vulnerabilidade	R$	622.295,78	R$	622.295,78	R$	622.295,78	R$	622.295,78
Serviços contínuos de pentest	R$	920.623,71	R$	920.623,71	R$	920.623,71	R$	920.623,71
Serviços contínuos de revisão de código fonte	R$	608.166,55	R$	608.166,55	R$	608.166,55	R$	608.166,55
Serviços contínuos de modelagem de ameaças e avaliação de riscos	R$	263.589,67	R$	263.589,67	R$	263.589,67	R$	263.589,67
Banco de horas de serviço de pentest	R$	608.166,55	R$	608.166,55	R$	608.166,55	R$	608.166,55
Custo Total do Ano	R$	3.022.842,26	R$	3.022.842,26	R$	3.022.842,26	R$	3.022.842,26
CTO da Solução							R$	12.091.369,03

De outra forma, o resultado consolidado do custo anualizado do serviço a ser contratado a partir da estima de preço calculada pode ser identificado na Tabela 13.

Tabela 13 TCO anualizado consolidado da contratação a partir da estimativa de preço resultante da pesquisa de preços.

Descrição da solução	Estimativa de TCO ao longo dos anos				Total
	2027	2028	2029	2030	

Solução 1 - Contratação de serviços contínuos	R$ 3.022.842,26	R$ 3.022.842,26	R$ 3.022.842,26	R$ 3.022.842,26	R$ 12.091.369,03

13. Estimativa de custo total da contratação

Valor (R$): 12.091.369,03

Consolidando os valores da Tabela 12, é possível consolidar na Tabela 14 os valores unitários dos serviços desejados associados aos quantitativos estimados para o projeto. Com isso, o projeto adota como estimativa de valor global do projeto o valor de **R$ 12.091.369,03**.

Tabela 14Memória de cálculo para estimativa de valor unitário dos serviços a serem contratados com base no valor calculado a partir da estimativa de preços.

Subitem	Descrição	Quantidade	Valor Unitário	Valor Total
1	Serviço contínuo de gestão de vulnerabilidades (meses)	48	R$ 51.857,98	R$ 2.489.183,10
2	Serviço contínuo de testes de invasão (pentesting) (meses)	48	R$ 76.718,64	R$ 3.682.494,85
3	Serviço contínuo de inspeção de código fonte (meses)	48	R$ 50.680,55	R$ 2.432.666,20
4	Banco de horas de testes de invasão (horas)	4000	R$ 263,59	R$ 1.054.358,69
5	Serviço contínuo de modelagem de ameaças e mensuração de riscos cibernéticos (meses)	48	R$ 50.680,55	R$ 2.432.666,20
Total				R$ 12.091.369,03

14. Justificativa técnica da escolha da solução

A alternativa selecionada - contratação de serviços contínuos especializados de gestão de vulnerabilidades, testes de invasão, inspeção manual de código-fonte e modelagem de ameaças /mensuração de riscos, mostrou-se a única capaz de atender integralmente aos requisitos de negócio, tecnológicos e operacionais identificados ao longo deste ETP.

Do ponto de vista técnico, a escolha fundamenta-se na necessidade de preservar continuidade, profundidade e sinergia entre os processos que compõem o ciclo de segurança cibernética do BCB. Conforme demonstrado nas análises anteriores, tais processos são interdependentes: vulnerabilidades detectadas alimentam avaliações de risco; modelos de ameaça subsidiam testes de invasão e análises de código; e os resultados dos pentests retroalimentam o monitoramento contínuo. A prestação fragmentada ou por escopos isolados quebraria essa cadeia de retroalimentação técnica, gerando perda de contexto, menor precisão analítica e aumento de retrabalho. A solução contínua, ao contrário, permite retenção de conhecimento institucional, acúmulo de domínio arquitetural e maior qualidade das entregas.

Além disso, a grande heterogeneidade do ambiente tecnológico do BCB, com milhares de ativos, centenas de softwares distintos, grande volume de código próprio e ritmo constante de implantação de soluções, exige um modelo de prestação capaz de operar de forma incremental, adaptativa e sem descontinuidade. Serviços contínuos são, portanto, indispensáveis para manter a tempestividade das análises e evitar riscos operacionais decorrentes de filas represadas, janelas de exposição a vulnerabilidades prolongadas ou eventuais gargalos de capacidade de resposta.

14.1 **DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS**

A lei 14.133/2021 estabelece, como diretriz geral, o parcelamento das contratações com vistas à ampliação da competitividade e à obtenção de melhores condições para a administração, conforme disposto em seu artigo nº 40, parágrafo segundo.

Entretanto, o terceiro parágrafo do mesmo artigo apresenta exceções para tal diretriz quanto o parcelamento do objeto se mostrar tecnicamente inviável ou desvantajoso, notadas nas seguintes hipóteses: (Inciso I) “A economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor.”; (Inciso II) “O objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.”.

No presente caso, a contratação proposta caracteriza-se como objeto único e integrado, composto por serviços técnicos especializados de segurança cibernética que são intrinsecamente interdependentes, a saber: gestão de vulnerabilidades, testes de invasão, inspeção manual de código-fonte e modelagem de ameaças e avaliação de riscos. Tais serviços não se desenvolvem isoladamente, ao contrário, os insumos produzidos por cada atividade alimentam e qualificam as demais, formando um ciclo contínuo de retroalimentação técnica.

Por exemplo, modelos de ameaça e avaliações de risco subsidiam a definição de escopos e profundidade de testes de invasão e inspeções de código fonte, bem como priorizações para a gestão de vulnerabilidades; resultados de pentests e inspeções de código fonte também oferecem critérios de priorização para o serviço de gestão de vulnerabilidades; finalmente, o monitoramento contínuo de vulnerabilidades orienta avaliações extraordinárias de risco e revisões de arquitetura.

O parcelamento do objeto em contratos ou itens independentes introduziria risco relevante à coerência metodológica, à continuidade analítica e à qualidade técnica das entregas, além de potencializar conflitos de responsabilidade entre fornecedores distintos, dificultar a rastreabilidade de riscos cibernéticos e comprometer a retenção de conhecimento sobre a arquitetura, os padrões de desenvolvimento e os fluxos operacionais dos sistemas do BCB.

Além disso, a fragmentação da contratação resultaria em perda de economia de escala e aumento do custo de gestão contratual, pois, ao demandar múltiplos contratos, implicaria em gerir múltiplos processos de fiscalização, então demandando um maior esforço de coordenação técnica por parte da Administração, sem qualquer ganho proporcional de eficiência ou competitividade.

Diante deste contexto, conclui-se que o parcelamento do objeto não se mostra tecnicamente recomendável, enquadrando-se nas exceções previstas nos incisos I e II do terceiro parágrafo do Art. 40 da lei 14.133/2021. Assim, a contratação integrada dos serviços especializados de segurança cibernética apresenta-se como a alternativa mais adequada sob a ótica técnica, operacional e de gestão de riscos.

15. Justificativa econômica da escolha da solução

A alternativa selecionada se demonstrou capaz de suprir as limitações de quadro reduzido da instituição. A contratação de serviços contínuos especializados apresenta custo global condizente com o orçamento reservado para o propósito.

O modelo de prestação de serviços contínuos também se mostrou mais eficiente economicamente do que a contratação por escopos isolados. Este último, além de tecnicamente inadequado, implicaria perda de escala, necessidade constante de aculturamento técnico de equipes distintas a cada demanda e maior risco de retrabalho devido à ausência de continuidade e retenção de conhecimento. Assim, o custo de transação associado ao modelo por escopo seria expressivamente mais elevado, sem entregar proporcional ganho técnico.

Desse modo, a solução escolhida maximiza a economicidade ao proporcionar a melhor relação entre custo e benefício: reduz o impacto financeiro para a instituição, preserva a continuidade operacional dos processos de segurança cibernética e evita o custo oculto decorrente da sobrecarga ou da reorientação de servidores para atividades especializadas que ultrapassam a disponibilidade atual da força de trabalho.

15.1 **O PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS**[DD1]

Sob a ótica econômica, o parcelamento da contratação em múltiplos itens ou contratos distintos não se mostra vantajoso para a Administração. Ainda que tecnicamente viável em abstrato, tal fragmentação implicaria aumento relevante dos custos de transação associados à contratação, gestão e fiscalização contratual.

A divisão do objeto demandaria a condução de gestão simultânea de diversos contratos, com consequente ampliação do esforço administrativo, do custo de fiscalização, da complexidade de coordenação entre fornecedores e do risco de sobreposição de atividades ou lacunas de cobertura entre os serviços contratados.

Ademais, a contratação integrada possibilita a captura de economias de escala, tanto na precificação dos serviços quanto na diluição de custos fixos da contratada, tais como estrutura técnica, gestão, capacitação e aculturamento ao ambiente institucional do BCB. O parcelamento, ao contrário, tenderia a elevar os preços unitários dos serviços, uma vez que cada fornecedor incorporaria integralmente seus custos indiretos e margens de risco.

Dessa forma, sob o prisma estritamente econômico, conclui-se que o parcelamento da contratação não se revela vantajoso, uma vez que resultaria em aumento de custos diretos e indiretos para a Administração, sem entrega proporcional de benefícios financeiros ou operacionais.

16. Benefícios a serem alcançados com a contratação

A contratação proposta proporcionará benefícios técnicos, operacionais, estratégicos e econômicos diretamente relacionados às necessidades institucionais identificadas neste ETP. Esses benefícios contribuem para o fortalecimento da resiliência cibernética do Banco Central do Brasil, a continuidade das operações críticas e o cumprimento dos objetivos estratégicos estabelecidos no PDTIC, especialmente no que tange à governança, segurança e integridade das soluções de TIC.

Entre os principais benefícios esperados, destacam-se:

- **Aumento da capacidade de resposta a vulnerabilidades**
  A prestação contínua de serviços de gestão de vulnerabilidades permitirá ao BCB reagir tempestivamente às novas vulnerabilidades publicadas, reduzindo janelas de exposição e evitando riscos operacionais decorrentes da crescente complexidade do ambiente tecnológico e do volume acelerado de CVEs reportadas anualmente.
- **Melhoria da qualidade técnica das avaliações e maior precisão analítica**
  A manutenção de equipe dedicada favorece o acúmulo de conhecimento sobre a arquitetura, padrões de desenvolvimento, integrações internas e características operacionais dos sistemas do BCB. Esse conhecimento contínuo resulta em entregas mais consistentes, com maior profundidade técnica e menor retrabalho.
- **Sinergia e integração entre os processos de segurança cibernética**
  A integração entre monitoramento de vulnerabilidades, modelagem de ameaças, testes de invasão e inspeção de código fortalece o ciclo completo de proteção, permitindo que os resultados de um processo alimentem e aprimorem os demais, aumentando a maturidade operacional da área de segurança cibernética.
- **Aumento da eficiência organizacional e preservação de recursos internos**
  A contratação reduz a sobrecarga sobre o quadro funcional e evita o redirecionamento de servidores a tarefas especializadas que exigem grande dedicação temporal e conhecimento técnico avançado. Com isso, o BCB preserva sua força de trabalho para outras atribuições estratégicas, prevenindo gargalos e reduzindo o risco de degradação de atividades essenciais.

- **Escalabilidade operacional e capacidade de adaptação à demanda**
  A disponibilidade de serviços contínuos e de banco de horas para pentest permite absorver variações na demanda institucional sem comprometer prazos, cronogramas de implantação de soluções e rotinas internas de segurança.
- **Melhoria da conformidade com boas práticas, regulamentos e normas internas**
  A contratação permite aderência mais ampla às diretrizes da IN SGD/ME nº 94/2022, ao manual POSTI, às necessidades do PMARC e às melhores práticas de segurança da informação aplicáveis ao setor público e ao setor financeiro.
- **Otimização de custos e melhor relação custo-benefício**
  A análise de TCO demonstrou que a solução contínua apresenta custo significativamente inferior ao do esforço interno necessário para realizar as mesmas atividades. Além disso, a redução de retrabalho, o ganho de escala e a previsibilidade contratual reforçam a economicidade da alternativa selecionada.
- **Contribuição direta aos objetivos estratégicos do BCB**
  A contratação fortalece especialmente os objetivos estratégicos OE1 (Aprimorar a governança, processos internos e gestão de recursos de TIC) e OE7 (Promover segurança cibernética e privacidade digital), conforme previsto no PDTIC vigente.

17. Providências a serem Adotadas

Não há providências a serem adotadas previstas para a instituição receber a solução escolhida, pois os instrumentos de fiscalização e de avaliação do modelo de execução de contrato puderam ser elaborados durante a elaboração das documentações relativas a este planejamento de contratação. Além disso, os serviços contratados serão integrados a processos já estabelecidos e praticados internamente na instituição, então não havendo nenhum esforço de elaboração de novos processos operacionais para serem operados pela Contratada.

18. Referências

1. MITRE CORPORATION. CVE Metrics — Published CVE Records by Year. Common Vulnerabilities and Exposures (CVE). Disponível em: https://www.cve.org/about/Metrics. Acesso em: 23 de Fevereiro de 2026.
2. CVE DETAILS. Number of security vulnerabilities by CVSS scores. cvedetails.com, [s. l.], 2025. Disponível em: https://www.cvedetails.com/cvss-score-distribution.php. Acesso em : 23 de fevereiro de 2026.
3. BRASIL. Decreto nº 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Brasília, DF, 16 set. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11200.htm. Acesso em: 05 de março de 2026.
4. BRASIL. Ministério da Economia. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do SISP do Poder Executivo Federal. Diário Oficial da União, Brasília, DF, 29 dez. 2022, Seção 1, p. 114. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-sgd/me-n-94-de-23-de-dezembro-de-2022-454510332. Acesso em: 05 de março de 2026.
5. BRASIL. Lei nº 14.133, de 1º de abril de 2021. Estabelece normas gerais de licitação e contratação para as Administrações Públicas. Diário Oficial da União, Brasília, DF, 1º abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14133.htm. Acesso em: 05 de março de 2026.

6. OWASP Foundation. OWASP Code Review Guide – Version 2.0. [S.l.]: OWASP, 2017. Disponível em: https://owasp.org/www-project-code-review-guide/assets/OWASP_Code_Review_Guide_v2.pdf. Acesso em: 05 de março de 2026.
7. INSTITUTO DE PESQUISA ECONÔMICA APLICADA (IPEA). Índice de Custo da Tecnologia da Informação (ICTI): índice (dez. 2012 = 100) – Série DIMAC_ICTI3. IPEAdata, atualização de 04 fev. 2026. Disponível em: https://www.ipeadata.gov.br/ExibeSerie.aspx?serid=30020. Acesso em: 05 de março de 2026.
8. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2019. Brasília, DF: BCB, 2019. Disponível em: https://www.bcb.gov.br/publicacoes/rig-nossaforca. Acesso em: 05 de março de 2026.
9. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2020. Brasília, DF: BCB, 2020. Disponível em: https://www.bcb.gov.br/publicacoes/rig20-nossaforca. Acesso em: 05 de março de 2026.
10. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2021. Brasília, DF: BCB, 2021. Disponível em: https://www.bcb.gov.br/publicacoes/rig21-nossaforcaerecursos. Acesso em: 05 de março de 2026.
11. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2022. Brasília, DF: BCB, 2022. Disponível em: https://www.bcb.gov.br/publicacoes/rig22-nossaforcaerecursos. Acesso em: 05 de março de 2026.
12. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2023. Brasília, DF: BCB, 2023. Disponível em: https://www.bcb.gov.br/publicacoes/rig23-nossaforcaerecursos. Acesso em: 05 de março de 2026.
13. BANCO CENTRAL DO BRASIL. Relatório Integrado do Banco Central do Brasil 2024. Brasília, DF: BCB, 2024. Disponível em: https://www.bcb.gov.br/content/publicacoes/rig/RIG_2024.pdf. Acesso em: 05 de março de 2026.
14. BANCO CENTRAL DO BRASIL. Servidores e carreira. Brasília, DF: BCB, 2026. Disponível em: https://www.bcb.gov.br/acessoinformacao/carreira. Acesso em: 05 de março de 2026.
15. TESOURO NACIONAL. Portal de Custos do Governo Federal. Brasília, DF: Tesouro Nacional, 2026. Disponível em: https://www.tesourotransparente.gov.br/visualizacao/portal-de-custos-do-governo-federal. Acesso em: 05 de março de 2026.
16. BRASIL. Ministério da Fazenda. Secretaria do Tesouro Nacional. Manual do Portal de Custos do Governo Federal. Brasília, DF: STN, [s.d.]. Disponível em: https://thot-arquivos.tesouro.gov.br/publicacao/52200. Acesso em: 05 de março de 2026.
17. CENTER FOR INTERNET SECURITY (CIS). CIS RAM – Risk Assessment Method. CIS, 2025. Disponível em: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method. Acesso em: 05 de março de 2026.
18. LI, Kaixuan et al. Comparison and evaluation on static application security testing (sast) tools for java. In: Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2023. p. 921-933.
19. BANCO CENTRAL DO BRASIL. Plano Diretor de Tecnologia da Informação e Comunicação – PDTI 2020–2025. Brasília, DF: BCB, 2020. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/pdti_docs/PDTI-2020-2025.pdf. Acesso em: 05 de março de 2026.
20. BRASIL. Edital nº 1/2024. Publicado pelo órgão responsável no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/04203025000143/compras/2024/1/arquivos/2. Acesso em: 05 de março de 2026.
21. BRASIL. Edital nº 25/2024. Publicado pelo órgão responsável (CNPJ 27.165.745/000167) no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/27165745000167/compras/2024/212/arquivos/2. Acesso em: 05 de março de 2026.
22. BRASIL. Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba (CODEVASF). Edital nº 90.078/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00399857000126/compras/2025/417/arquivos/2. Acesso em: 05 de março de 2026.

23. BRASIL. Fundação do ABC (FMABC). Edital nº 90.007(5)/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00394585000171/compras/2024/314/arquivos/2. Acesso em: 05 de março de 2026.
24. BRASIL. Tribunal de Justiça do Estado de São Paulo (TJSP). Edital nº 90.088/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/51174001000193/compras/2025/153/arquivos/1. Acesso em: 05 de março de 2026.
25. BRASIL. Companhia de Desenvolvimento de Maricá (CODEMAR). Edital nº 90.009/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/20009382000121/compras/2025/8/arquivos/1. Acesso em: 05 de março de 2026.
26. BRASIL. Agência Reguladora Intermunicipal de Saneamento (ARIS). Edital nº 006/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/11400360000105/compras/2025/38/arquivos/1. Acesso em: 05 de março de 2026.
27. BRASIL. Tribunal de Justiça Militar do Estado de São Paulo (TJMSP). Edital nº 90.023/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/60265576000102/compras/2025/49/arquivos/1. Acesso em: 05 de março de 2026.
28. BRASIL. Departamento Nacional de Infraestrutura de Transportes (DNIT). Edital nº 90.253/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/04892707000100/compras/2025/403/arquivos/4. Acesso em: 05 de março de 2026.
29. BRASIL. CGRL – órgão responsável (CNPJ 37.753.638/000103). Edital nº 10/2023. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/37753638000103/compras/2023/31/arquivos/1. Acesso em: 05 de março de 2026.
30. BRASIL. Tribunal de Justiça do Estado de Belo Horizonte (TJBH). Edital nº 90.048/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/13100722000160/compras/2024/72/arquivos/3. Acesso em: 05 de março de 2026.
31. BRASIL. Prefeitura Municipal de Macaé. Edital nº 90.047/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/29115474000160/compras/2025/239/arquivos/1. Acesso em: 05 de março de 2026.
32. BRASIL. Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). Edital nº 54/2023. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00531954000120/compras/2023/140/arquivos/1. Acesso em: 05 de março de 2026.
33. BRASIL. Polícia Civil do Distrito Federal (PCDF). Edital nº 90.008/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/37115482000135/compras/2025/12/arquivos/3. Acesso em: 05 de março de 2026.
34. BRASIL. Tribunal de Contas do Estado do Rio de Janeiro (TCERJ). Edital nº 90.028/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00414607000118/compras/2024/101/arquivos/1. Acesso em: 05 de março de 2026.
35. BRASIL. Departamento Estadual de Trânsito de Rondônia (DETRANRO). Edital nº 90.007/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00394585000171/compras/2024/314/arquivos/2. Acesso em: 05 de março de 2026.

36. BRASIL. Órgão responsável (CNPJ 07.237.373/000120). Edital nº 90.068/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/07237373000120/compras/2025/59/arquivos/1. Acesso em: 05 de março de 2026.
37. BRASIL. Secretaria de Estado da Fazenda de Santa Catarina (SEFAZSC). Edital nº 30/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/82951310000156/compras/2025/53/arquivos/1. Acesso em: 05 de março de 2026.
38. BRASIL. Governo do Estado do Rio de Janeiro. Edital nº PERP20/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/42498600000171/compras/2025/6615/arquivos/1. Acesso em: 05 de março de 2026.
39. BRASIL. Ministério Público da União (MPU). Edital nº 90.025/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/26989715000102/compras/2025/2576/arquivos/1. Acesso em: 05 de março de 2026.
40. BRASIL. Governo do Estado de São Paulo. Edital nº 90.038/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/46374500000194/compras/2025/315/arquivos/1. Acesso em: 05 de março de 2026.
41. BRASIL. Empresa de Tecnologia da Informação e Comunicação do Estado do Pará (PRODEPA). Edital nº 90.005/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/05054861000176/compras/2024/811/arquivos/1. Acesso em: 05 de março de 2026.
42. BRASIL. Tribunal de Justiça do Estado de Rondônia (TJRO). Edital nº 90.086/2025. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/04293700000172/compras/2025/134/arquivos/2. Acesso em: 05 de março de 2026.
43. BRASIL. Tribunal Superior Eleitoral (TSE). Edital nº 60/2023. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00509018000113/compras/2023/2139/arquivos/1. Acesso em: 05 de março de 2026.
44. BRASIL. Tribunal de Contas do Estado de Minas Gerais (TCEMG). Edital nº194/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/21154877000107/compras/2024/174/arquivos/1. Acesso em: 05 de março de 2026.
45. BRASIL. Empresa de Pesquisa Energética (EPE). Edital nº90.018/2024. Publicado no Portal Nacional de Contratações Públicas – PNCP. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/06977747000180/compras/2024/20/arquivos/1. Acesso em: 05 de março de 2026.
46. OSTEC. Página inicial. Disponível em: https://www.ostec.com.br. Acesso em: 05 de março de 2026.
47. VANTICO. Página inicial. Disponível em: https://vantico.com.br. Acesso em: 05 de março de 2026.
48. LOPRESTISEC. Página inicial. Disponível em: https://loprestisec.com.br. Acesso em: 05 de março de 2026.
49. SKYONE. Página inicial. Disponível em: https://www.skyone.solutions. Acesso em: 05 de março de 2026.
50. TEMPEST SECURITY INTELLIGENCE. Página inicial. Disponível em: https://www.tempest.com.br. Acesso em: 05 de março de 2026.
51. CLAVIS SEGURANÇA DA INFORMAÇÃO. Página inicial. Disponível em: https://clavis.com.br. Acesso em: 05 de março de 2026.
52. ENYGMA TECNOLOGIA. Página inicial. Disponível em: https://enygma.tec.br. Acesso em: 05 de março de 2026.
53. DIA ZERO SECURITY. Página inicial. Disponível em: https://www.diazerosecurity.com.br. Acesso em: 05 de março de 2026.
54. SECURE TECNOLOGIA. Página inicial. Disponível em: https://www.securetecnologia.com.br. Acesso em: 05 de março de 2026.

55. BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. Portaria STI/MP nº 46, de 28 de setembro de 2016. Dispõe sobre a disponibilização de Software Público Brasileiro e dá outras providências. Disponível em: https://www.gov.br/governodigital/pt-br/plataformas-e-servicos-digitais/software-publico/portaria-46.pdf. Acesso em: 05 de março de 2026.
56. BRASIL. Ministério da Economia. ÁGATHA – Sistema de Gestão de Riscos e Integridade. Portal do Software Público Brasileiro. Disponível em: https://softwarepublico.gov.br/social/agatha. Acesso em: 05 de março de 2026.
57. CENTER FOR INTERNET SECURITY. CIS Critical Security Controls: Version 8.1. June 2024. Acesso em: 11 mar. 2026.
58. UNITED STATES. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 80053, Revision 5. Gaithersburg, MD: NIST, 2020. Disponível em: https://csf.tools/reference/nist-sp-800-53/r5/. Acesso em: 11 mar. 2026.
59. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO/IEC, 2022.
60. JERIMY, Paul. *Security Certification Roadmap*. Paul Jerimy Media, [s. l.], [s. d.]. Disponível em: https://pauljerimy.com/security-certification-roadmap/. Acesso em: 16 mar. 2026.
61. FUNDAÇÃO MUNICIPAL ABC (FMABC). Edital nº 90005/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/46379400000150/compras/2025/64/arquivos/1. Acesso em: 24 abr. 2026.
62. FUNDAÇÃO MUNICIPAL ABC (FMABC). Edital nº 90007/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/57571275000798/compras/2025/2/arquivos/2. Acesso em: 24 abr. 2026.
63. TRIBUNAL DE JUSTIÇA MILITAR DE SÃO PAULO (TJMSP). Edital nº 90023/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/60265576000102/compras/2025/49/arquivos/1. Acesso em: 24 abr. 2026.
64. PREFEITURA MUNICIPAL DE TAUBATÉ. Edital nº 247/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/45176005000108/compras/2025/489/arquivos/1. Acesso em: 24 abr. 2026.
65. CONSELHO FEDERAL DE MEDICINA (CFM). Edital nº 90024/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/33583550000130/compras/2025/176/arquivos/1. Acesso em: 24 abr. 2026.
66. COMPANHIA DE DESENVOLVIMENTO DOS VALES DO SÃO FRANCISCO E DO PARNAÍBA (CODEVASF). Edital nº 90078/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/00399857000126/compras/2025/417/arquivos/2. Acesso em: 24 abr. 2026.
67. SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL (SENAC). Edital nº 90054/2024. 2024. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/03965450000107/compras/2024/11/arquivos/2. Acesso em: 24 abr. 2026.
68. TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO (TJSP). Edital nº 90088/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/51174001000193/compras/2025/153/arquivos/1. Acesso em: 24 abr. 2026.
69. TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA (TJBA). Edital nº 90048/2024. 2024. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/13100722000160/compras/2024/72/arquivos/3. Acesso em: 24 abr. 2026.
70. COMPANHIA DE DESENVOLVIMENTO DE MARICÁ (CODEMAR). Edital nº 90009/2025. 2025. Disponível em: https://pncp.gov.br/pncp-api/v1/orgaos/20009382000121/compras/2025/8/arquivos/1. Acesso em: 24 abr. 2026.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

A declaração de viabilidade apresentada fundamenta-se na análise conjunta dos aspectos técnicos, funcionais e econômicos consolidados ao longo deste ETP. A alternativa selecionada: “contratação de serviços contínuos especializados de gestão de vulnerabilidades, testes de invasão, inspeção manual

de código-fonte e modelagem de ameaças/mensuração de riscos", mostrou-se a única capaz de atender integralmente às necessidades institucionais, superar os problemas identificados e mitigar os riscos operacionais decorrentes das limitações atuais de capacidade interna.

Do ponto de vista **técnico**, a solução escolhida permite preservar a continuidade e a sinergia entre processos interdependentes do ciclo de segurança cibernética, garantindo maior profundidade analítica, consistência das avaliações e tempestividade na detecção e tratamento de vulnerabilidades. A alternativa por escopo, além de inadequada tecnicamente, não atende requisitos essenciais de escalabilidade, integração entre atividades e retenção de conhecimento. Já a alternativa baseada exclusivamente em esforço interno revelou-se insuficiente para cumprir a regularidade, profundidade e abrangência exigidas pela demanda institucional.

Sob a ótica da **eficácia**, a contratação assegura que os serviços necessários serão executados com a qualidade, frequência e abrangência requeridas, eliminando gargalos e reduzindo janelas de exposição a ameaças cibernéticas. Quanto à **efetividade**, a solução proporciona os resultados estratégicos esperados ao fortalecer a resiliência cibernética do Banco Central, apoiar processos críticos e garantir que novas soluções tecnológicas sejam avaliadas de forma consistente e tempestiva.

Em termos de **eficiência**, a solução contínua oferece ganhos claros ao permitir maior produtividade, especialização e aproveitamento do conhecimento acumulado pela equipe dedicada, reduzindo retrabalho e aumentando a qualidade das entregas. A análise de **economicidade**, consolidada no cálculo de TCO, demonstra que o custo total da contratação é significativamente inferior ao custo econômico do atendimento da demanda exclusivamente por servidores internos, além de ser mais vantajoso do que modelos de execução descontinuados ou fragmentados.

Assim, a alternativa selecionada demonstra aderência integral às necessidades institucionais, aos requisitos técnicos levantados, às diretrizes normativas aplicáveis e aos objetivos estratégicos da organização. Diante desse conjunto de evidências, conclui-se que a contratação proposta é viável, justificável e representa a melhor relação entre custo e benefício para o Banco Central do Brasil.

20. 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

DANILO DIAS

Integrante Requisitante

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

IURI SOUSA DA ROCHA

Integrante Administrativo