INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Abril 2026

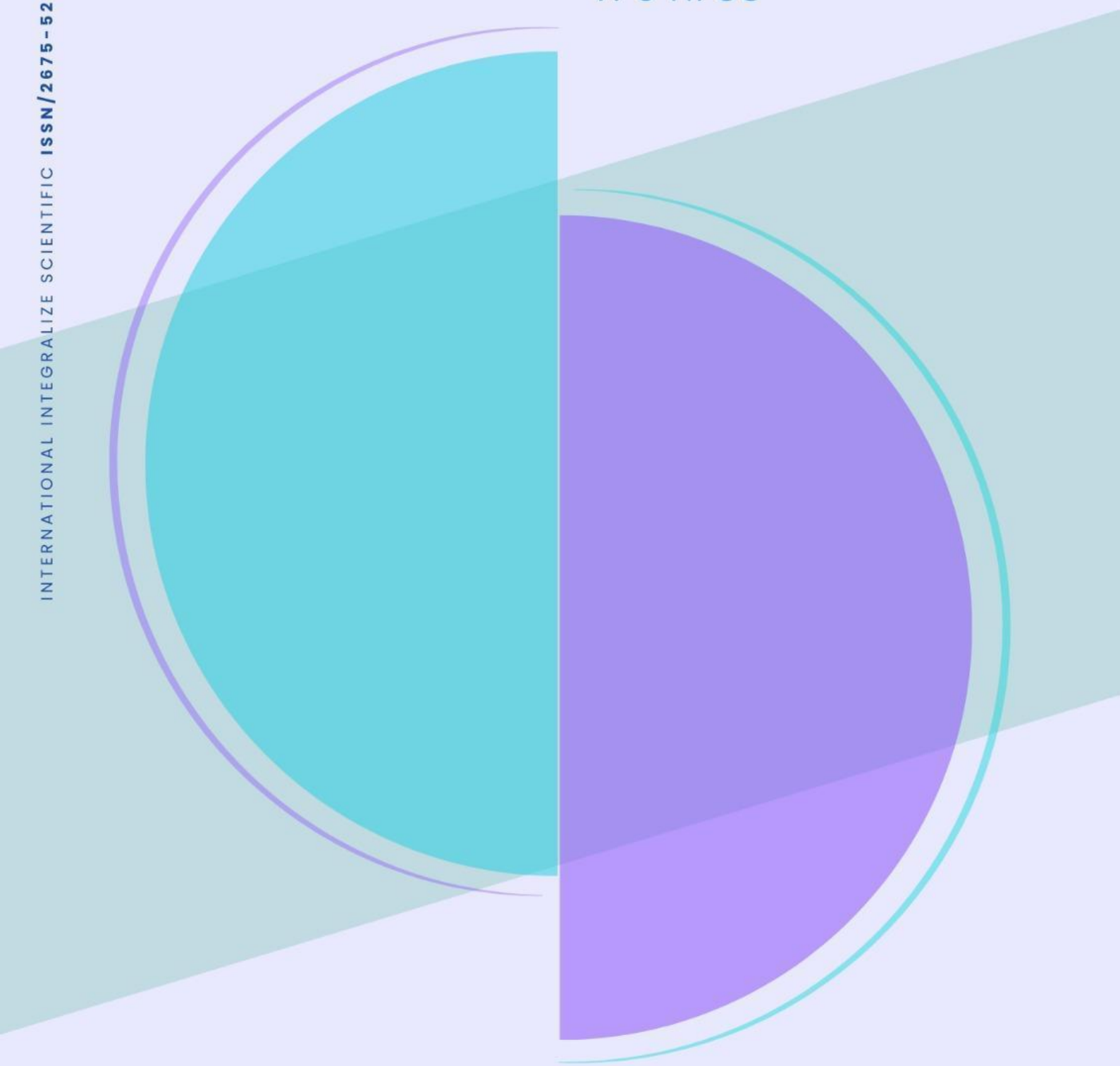
v. 6 n. 58

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520

INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Abril 2026
v. 6 n. 58

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520



iiscientific.com

APRESENTAÇÃO

A International Integralize Scientific configura-se como um periódico científico mensal dedicado à difusão rigorosa e qualificada do conhecimento acadêmico. Com publicações predominantemente em língua portuguesa e contribuições consistentes em inglês e espanhol, a revista consolida-se como um espaço editorial multicultural, orientado ao diálogo científico internacional e ao fortalecimento da produção intelectual brasileira no cenário global.

Alinhada a elevados critérios de avaliação acadêmica, a revista privilegia a publicação de artigos inéditos de discentes e docentes provenientes de distintas áreas do saber, reconhecendo a ciência como campo plural e interdisciplinar. Cada manuscrito submetido passa por criteriosa análise técnico-científica em regime de avaliação por pares, assegurando integridade metodológica, consistência teórica e relevância social dos resultados apresentados. Dessa forma, a International Integralize Scientific reafirma seu compromisso institucional com a circulação responsável do conhecimento e com o fortalecimento da cultura de pesquisa.

Sua missão institucional consiste em promover a publicação e a disseminação de pesquisas inovadoras que contribuam efetivamente para o avanço científico e tecnológico, estimulando a reflexão crítica e o desenvolvimento de novas abordagens investigativas. A revista persegue a visão de consolidar-se como referência de credibilidade e excelência acadêmica no contexto internacional, valorizando a produção científica que se ancora em evidências sólidas, metodologias reconhecidas e padrões éticos elevados.

A governança editorial do periódico opera em plataforma Open Journal Systems (OJS), garantindo transparência processual, rastreabilidade, interoperabilidade com bases internacionais e aderência às melhores práticas em editoração científica. A revista possui registro ISSN nas versões impressa e digital e atribui Digital Object Identifier (DOI) a todas as publicações, mediante associação ativa à Crossref, assegurando autenticidade, persistência e ampla citabilidade internacional. Sua atuação editorial mantém alinhamento às boas práticas recomendadas por organizações científicas de referência e aos princípios éticos, técnicos e normativos que orientam a gestão de periódicos acadêmicos qualificados, incluindo diretrizes consolidadas no âmbito da normalização internacional.

Os valores que regem sua atuação editorial fundamentam-se no rigor científico, na ética acadêmica e na promoção de um ecossistema plural de saberes. A diversidade disciplinar, a integridade intelectual, a inovação, o impacto social da ciência e a construção de redes colaborativas entre pesquisadores de diferentes nacionalidades constituem pilares estruturantes do periódico. Ao incentivar a interlocução entre centros de pesquisa, universidades e comunidades científicas, a International Integralize Scientific contribui para o desenvolvimento de uma ciência aberta ao diálogo, orientada à melhoria contínua e sensível às demandas contemporâneas.

Sua periodicidade regular, o compromisso com padrões editoriais elevados e a interlocução permanente com autores e avaliadores qualificados reforçam a credibilidade da revista como veículo legítimo de disseminação científica. Trata-se, assim, de um espaço editorial que acolhe a investigação acadêmica com seriedade, estimulando trajetórias de produção intelectual consistente, ética e socialmente relevante.

Ao posicionar-se como ponte entre diferentes culturas, idiomas e tradições científicas, a International Integralize Scientific reafirma o papel estratégico dos periódicos acadêmicos no fortalecimento da ciência global e na promoção de um conhecimento capaz de transformar realidades, ampliar horizontes e projetar pesquisadores brasileiros e internacionais em um ambiente científico de excelência.

Expediente Editorial

A Revista International Integralize Scientific é um periódico científico mensal dedicado à promoção e disseminação de conhecimento acadêmico de alta qualidade, orientado por rigor metodológico e compromisso ético. Seu propósito central consiste em oferecer um espaço de visibilidade qualificada para pesquisas inéditas, contribuindo para o fortalecimento do debate científico e para o desenvolvimento contínuo das diversas áreas do saber. Ao assegurar processos criteriosos de avaliação e seleção editorial, o periódico reafirma sua vocação institucional de fomentar o pensamento crítico, incentivar o intercâmbio intelectual e apoiar a formação de novas gerações de pesquisadores.

Características do Periódico

Periodicidade:
Mensal
Idiomas de Publicação:
Português, Inglês e Espanhol
Plataforma Editorial:
Open Journal Systems (OJS)
Registro Internacional:
SSN 3085-654X
Identificação Digital:
DOI registrado e associado à Crossref

Contato Editorial

Para esclarecimentos, submissões, parcerias institucionais ou orientações relacionadas ao processo editorial, a equipe técnica encontra-se à disposição através do e-mail:
publicacao@iiscientific.com

Endereço Institucional

Florianópolis – Santa Catarina – Brasil
Rodovia SC-401, Bairro Saco Grande
CEP 88032-005

A International Integralize Scientific mantém atuação editorial orientada pelas boas práticas científicas internacionais, alinhada aos princípios de integridade acadêmica, transparência editorial e responsabilidade social do conhecimento. Seu corpo diretivo e técnico atua de maneira integrada para assegurar excelência, continuidade e relevância científica em cada edição publicada.

Corpo Editorial e Conselho de Revisores por Pares

A revista adota um rigoroso processo de avaliação científica por pares (peer review), conduzido preferencialmente no modelo doubleblind, garantindo anonimato entre autores e revisores durante o processo avaliativo, imparcialidade na emissão dos pareceres e excelência acadêmica na seleção dos manuscritos publicados.

A divulgação institucional do corpo editorial e dos revisores por pares não estabelece qualquer vinculação entre avaliadores e artigos específicos, preservando integralmente a confidencialidade e a integridade ética do processo de revisão.

Editora-Chefe

Profa. PhD Vanessa Sales

Equipe Editorial

Prof. PhD Hélio Sales Rios
Prof. Dr. Rafael Ferreira da Silva
Prof. Dr. Francisco Rogério Gomes da Silva
Prof. PhD Manoel Coracy Dias Saboia
Prof. Dr. Daniel LaiberBonadiman

Declaração de Transparência Editorial

O periódico mantém registro formal de todas as etapas do processo de avaliação científica, assegurando confidencialidade, ética, independência acadêmica e conformidade com o modelo doubleblindpeer review, no qual autores e revisores permanecem mutuamente anônimos durante o processo avaliativo.

Conselho de Revisores por Pares
(Peer Review Board)

O Conselho de Revisores por Pares é composto por pesquisadores com sólida formação acadêmica e reconhecida atuação científica. Os pareceres técnicos emitidos avaliam critérios de relevância científica, originalidade, consistência metodológica, contribuição teórica e adequação ética, fortalecendo o rigor e a credibilidade do periódico.

Pareceristas

Ciências da Educação
Dr. Carlos Mendonça
Dr. Marcelo Pertussatti
Dr. Ederson Renan Pacheco de Farias

Ciência da Saúde
Dr. Daniel Laiber
Dra. Luisa Bonadiman

Ciências Jurídicas
Dr. Avelino Thiago
Dr. James Melo de Sousa
Dr. Manoel Coracy

Educação Inclusiva
Dra. Fábia Roseana Souza Oliveira da Silva
Dra. Karla Roberta Melo de Vasconcellos

Tecnologia
Dr. Flávio Lopes
Dr. Geraldo Lúcio

Editor Gerente
Rayane Priscila Santos de Souza

Editores de Seção
Karolayne Luana de Oliveira Silva
Eloisa Bárbara Rodrigues Lima

Equipe de Produção Editorial
Reviane Francy Silva da Silveira
Priscila de Fátima Lima Schio
Lucas Teotônio Vieira

Editor Técnico
Balbino Júnior

Administrador do Sistema OJS
Vitor Santos

CIBERSEGURANÇA E PROTEÇÃO DE DADOS NO SETOR FINANCEIRO: ESTRATÉGIAS DE PREVENÇÃO E RESPOSTA A INCIDENTES EM BANCOS DIGITAIS NO BRASIL

CYBERSECURITY AND DATA PROTECTION IN THE FINANCIAL SECTOR: PREVENTION STRATEGIES AND INCIDENT RESPONSE IN DIGITAL BANKS IN BRAZIL

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS EN EL SECTOR FINANCIERO: ESTRATEGIAS DE PREVENCIÓN Y RESPUESTA A INCIDENTES EN BANCOS DIGITALES EN BRASIL

RESUMO

O artigo examina as estratégias de prevenção e resposta a incidentes cibernéticos nos bancos digitais brasileiros, investigando a articulação entre as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709/2018) e os requisitos de segurança cibernética estabelecidos pelo Banco Central do Brasil, em especial pela Resolução CMN n. 4.893/2021. O estudo aborda de que forma os bancos digitais estruturam suas políticas de cibersegurança, identificando os principais vetores de ataque, os instrumentos regulatórios disponíveis e as lacunas que comprometem a efetividade da proteção de dados no setor financeiro. Adota-se a pesquisa bibliográfica e documental de natureza qualitativa como procedimento metodológico, com análise crítica de legislação, normativas setoriais, relatórios técnicos de organizações nacionais e internacionais e literatura científica especializada. Os resultados indicam que a convergência regulatória entre a LGPD e a Resolução CMN n. 4.893/2021 cria uma estrutura dual de conformidade que impõe às instituições financeiras obrigações técnicas e jurídicas simultâneas, cujo cumprimento requer maturidade organizacional ainda não alcançada de forma uniforme entre os bancos digitais. Verifica-se, ainda, que os investimentos crescentes em tecnologia de segurança não se traduzem automaticamente em resiliência operacional, sendo necessária a construção de uma cultura de cibersegurança que integre pessoas, processos e tecnologia de forma sistêmica. O estudo contribui para o debate acadêmico sobre governança de risco digital no setor financeiro e oferece subsídios para o aprimoramento das políticas regulatórias de prevenção e resposta a incidentes em bancos digitais.

Palavras-chave: Cibersegurança; bancos digitais; proteção de dados; LGPD; resposta a incidentes.

ABSTRACT

This article examines prevention and incident response strategies against cyberattacks in Brazilian digital banks, investigating the articulation between the requirements of the General Personal Data Protection Law (LGPD, Law No. 13,709/2018) and the cybersecurity requirements established by the Central Bank of Brazil, particularly through Resolution CMN No. 4,893/2021. The study addresses how digital banks structure their cybersecurity policies, identifying the main attack vectors, available regulatory instruments, and gaps that compromise the effectiveness of data protection in the financial sector. Qualitative bibliographic and documentary research is adopted as the methodological procedure, with critical analysis of legislation, sectoral regulations, technical reports from national and international organizations, and specialized scientific literature. The results indicate that the regulatory convergence between the LGPD and Resolution CMN No. 4,893/2021 creates a dual compliance structure that imposes simultaneous technical and legal obligations on financial institutions, whose fulfillment requires organizational maturity not yet uniformly achieved among digital banks. Furthermore, it is found that growing investments in security technology do not automatically translate into operational resilience, requiring the construction of a cybersecurity culture that integrates people, processes, and technology in a systemic manner. The study contributes to the academic debate on digital risk governance in the financial sector and offers insights for improving regulatory policies on prevention and incident response in digital banks.

Keywords: Cybersecurity; digital banks; data protection; LGPD; incident response.

RESUMEN

El presente artículo examina las estrategias de prevención y respuesta a incidentes cibernéticos en los bancos digitales brasileños, investigando la articulación entre las exigencias de la Ley General de Protección de Datos Personales (LGPD, Ley n. 13.709/2018) y los requisitos de seguridad cibernética establecidos por el Banco Central de Brasil, especialmente mediante la Resolución CMN n. 4.893/2021. El estudio aborda cómo los bancos digitales estructuran sus políticas de ciberseguridad, identificando los principales vectores de ataque, los instrumentos regulatorios disponibles y las brechas que comprometen la efectividad de la protección de datos en el sector financiero. Se adopta la investigación bibliográfica y documental de naturaleza cualitativa como procedimiento metodológico, con análisis crítico de legislación, normativas sectoriales, informes técnicos de organizaciones nacionales e internacionales y literatura científica especializada. Los resultados indican que la convergencia regulatoria entre la LGPD y la Resolución CMN n. 4.893/2021 crea una estructura de cumplimiento dual que impone a las instituciones financieras obligaciones técnicas y jurídicas simultáneas, cuyo cumplimiento requiere una madurez organizacional aún no alcanzada de forma uniforme entre los bancos digitales. Se constata, asimismo, que las inversiones crecientes en tecnología de seguridad no se traducen automáticamente en resiliencia operacional, siendo necesaria la construcción de una cultura de ciberseguridad que integre personas, procesos y tecnología de forma sistémica. El estudio contribuye al debate académico sobre la gobernanza del riesgo digital en el sector financiero y ofrece subsidios para el perfeccionamiento de las políticas regulatorias de prevención y respuesta a incidentes en bancos digitales.

Palabras clave: Ciberseguridad; bancos digitales; protección de datos; LGPD; respuesta a incidentes.

1 INTRODUÇÃO

A ascensão dos bancos digitais no Brasil representa uma das transformações mais aceleradas e profundas do sistema financeiro nacional nas últimas décadas. Impulsionados pela expansão do acesso à internet, pelo advento do sistema de pagamentos instantâneos (Pix) e pelo arcabouço regulatório do open finance, esses novos atores financeiros passaram a concentrar expressivos volumes de dados pessoais e transacionais de milhões de brasileiros. Silva, Garcia Junior e Araújo (2022), em artigo publicado na Revista da Procuradoria-Geral do Banco Central, registram que as fintechs e os bancos digitais se estabeleceram como protagonistas da inclusão financeira no Brasil, ao oferecer serviços bancários simplificados, de baixo custo e totalmente mediados por plataformas digitais. Essa mudança estrutural, ao mesmo tempo em que democratiza o acesso a serviços financeiros, amplia significativamente a superfície de exposição às ameaças cibernéticas.

O cenário de risco associado à digitalização bancária é documentado por fontes de alta credibilidade. A Pesquisa Febraban de Tecnologia Bancária (Febraban/Deloitte, 2024) revelou que a segurança cibernética é prioridade estratégica para a totalidade dos bancos brasileiros entrevistados, com investimentos concentrados em arquitetura e infraestrutura de segurança, estratégias de detecção e resposta a ameaças e gestão de identidades e acessos. O mesmo relatório indica que

o orçamento total do setor bancário destinado à tecnologia deve atingir R$ 47,4 bilhões, com expressivo percentual destinado à proteção contra ameaças digitais. O FMI (2020), por sua vez, alertou que o número de ciberataques ao setor financeiro triplicou na última década e que o risco cibernético passou a representar uma ameaça sistêmica à estabilidade financeira global, não mais circunscrita ao domínio técnico das equipes de tecnologia da informação.

No plano normativo, o Brasil consolidou, ao longo dos últimos anos, um conjunto de diplomas legais e regulamentares que disciplinam as obrigações de segurança cibernética e proteção de dados no setor financeiro. A LGPD (Brasil, 2018) estabelece um regime geral de proteção de dados pessoais, com princípios, bases legais, obrigações de segurança e mecanismos de comunicação de incidentes aplicáveis a todas as organizações que tratam dados no país, incluindo os bancos digitais. A Resolução CMN n. 4.893/2021 (Brasil, 2021a) complementa esse quadro normativo ao impor especificamente às instituições financeiras autorizadas a funcionar pelo Banco Central a estruturação de políticas formais de segurança cibernética, planos de resposta a incidentes e requisitos para a contratação de provedores de serviços em nuvem. Motta e Rosa (2022), em artigo publicado na mesma Revista da PGBC, analisam como o open banking, ao ampliar o compartilhamento de dados financeiros entre instituições, intensifica os desafios de governança de dados e segurança cibernética impostos pela LGPD e pela regulação prudencial do BCB.

A justificativa para o presente estudo reside, em primeiro lugar, na lacuna acadêmica existente em relação às estratégias específicas de prevenção e resposta a incidentes nos bancos digitais brasileiros, em contraposição à literatura existente sobre o setor bancário tradicional. Os bancos digitais operam com modelos de negócio nativamente digitais, sem agências físicas, o que os torna integralmente dependentes de suas infraestruturas tecnológicas e os expõe a um perfil de risco cibernético distinto, marcado pela maior dependência de provedores de computação em nuvem e pela integração com múltiplos parceiros tecnológicos. Essa especificidade do modelo digital ainda carece de análise acadêmica aprofundada no contexto brasileiro, especialmente à luz das exigências regulatórias da LGPD e da Resolução CMN n. 4.893/2021.

Em segundo lugar, a justificativa desta pesquisa ancora-se na relevância prática do problema estudado. O Banco Central do Brasil registra mais de dois mil golpes financeiros por minuto no país, incluindo ligações fraudulentas, mensagens com cobranças indevidas e clonagem de cartões (NIC.br, 2020). Esse dado dimensiona a escala do problema e a urgência de estratégias efetivas de prevenção e resposta a incidentes que transcendam a mera conformidade formal com as normas regulatórias. Doneda (2020), em obra de referência sobre os fundamentos da LGPD, sublinha que a proteção de dados pessoais no Brasil só alcançará efetividade quando as organizações incorporarem os princípios legais em suas práticas operacionais cotidianas, e não apenas em suas políticas formais de privacidade. Esse imperativo é especialmente crítico para os bancos digitais, cujos clientes compartilham dados pessoais sensíveis de forma intensiva e contínua.

Em face do exposto, o presente artigo é orientado pelas seguintes perguntas norteadoras: De que forma o arcabouço regulatório brasileiro, especialmente a LGPD e a Resolução CMN n. 4.893/2021, disciplina as obrigações de prevenção e resposta a incidentes cibernéticos nos bancos digitais? Quais são os principais vetores de ataque cibernético identificados na literatura especializada e nos relatórios setoriais para o segmento de bancos digitais? Em que medida os investimentos crescentes em tecnologia de segurança se traduzem em maturidade efetiva de cibersegurança nas instituições financeiras digitais?

O objetivo geral deste estudo consiste em analisar as estratégias de prevenção e resposta a incidentes cibernéticos nos bancos digitais brasileiros, à luz da LGPD e da Resolução CMN n. 4.893/2021, identificando as principais lacunas de maturidade e os instrumentos regulatórios e técnicos disponíveis para seu enfrentamento. São estabelecidos três objetivos específicos: (i) caracterizar o marco regulatório de cibersegurança aplicável aos bancos digitais no Brasil; (ii) identificar os principais vetores de ataque e as estratégias de prevenção adotadas no setor financeiro digital; e (iii) analisar os desafios de conformidade simultânea com a LGPD e com a regulação prudencial do BCB nos bancos digitais.

O artigo estrutura-se em cinco seções. Após esta introdução, a segunda seção apresenta o referencial teórico, organizado em três subtópicos: o marco regulatório da cibersegurança e proteção de dados nos bancos digitais; os principais vetores de risco

cibernético no setor financeiro; e os modelos de governança de resposta a incidentes. A terceira seção descreve os procedimentos metodológicos adotados. A quarta seção apresenta e discute os resultados da pesquisa bibliográfica. A quinta e última seção expõe as considerações finais, com ênfase nas contribuições do estudo, nas limitações identificadas e nas recomendações para pesquisas futuras e políticas públicas.

2 REFERENCIAL TEÓRICO

2.1 Marco regulatório de cibersegurança e proteção de dados nos bancos digitais

A regulação bancária brasileira incorporou a dimensão cibernética de forma sistematizada com a edição da Resolução CMN n. 4.658/2018 pelo Banco Central, que pela primeira vez obrigou as instituições financeiras a estruturar políticas formais de segurança cibernética. Esse marco normativo foi sucedido e aprimorado pela Resolução CMN n. 4.893, de 26 de fevereiro de 2021, que revogou as disposições anteriores e introduziu exigências mais abrangentes de governança cibernética, gestão de riscos de terceiros e requisitos específicos para a contratação de serviços de computação em nuvem (Brasil, 2021a). Para os bancos digitais, cujo modelo de negócio é integralmente dependente de infraestruturas tecnológicas, essa norma representa o principal instrumento regulatório de disciplina do risco cibernético, impondo obrigações que vão da elaboração da política de segurança à prestação de contas periódica à alta administração.

A Resolução CMN n. 4.893/2021 adota uma abordagem regulatória baseada em princípios e proporcionalidade, exigindo que cada instituição financeira calibre suas obrigações ao seu porte, perfil de risco e modelo de negócio. Isso significa que os bancos digitais, por operarem em ambiente exclusivamente digital e processarem volumes expressivos de dados pessoais de clientes, precisam demonstrar controles de segurança robustos e compatíveis com o risco sistêmico que representam. A norma exige, especificamente: elaboração e divulgação de política de segurança cibernética; plano de ação e resposta a incidentes; testes periódicos de continuidade de negócios contemplando cenários de indisponibilidade por incidentes cibernéticos; e avaliação e monitoramento contínuo dos provedores de serviços de tecnologia da informação (Brasil, 2021a). Para a Resolução BCB n. 85/2021, que disciplina especificamente as

instituições de pagamento, aplicam-se requisitos análogos, adaptados às especificidades dessas entidades (Brasil, 2021b).

A LGPD (Brasil, 2018) constitui o segundo eixo normativo fundamental para os bancos digitais. Seus artigos 46 a 49 impõem aos controladores e operadores de dados a obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação indevida. O artigo 48 institui a obrigação de comunicação de incidentes de segurança que possam causar risco ou dano relevante aos titulares dos dados, a ser realizada à Autoridade Nacional de Proteção de Dados (ANPD) em prazo razoável. Bioni (2021) analisa como as múltiplas bases legais de tratamento de dados previstas na LGPD impõem aos bancos digitais o dever de mapear, documentar e justificar juridicamente cada operação de tratamento de dados de seus clientes, criando uma estrutura de compliance que vai muito além da simples elaboração de políticas de privacidade.

A constitucionalização da proteção de dados pessoais, operada pela Emenda Constitucional n. 115, de 10 de fevereiro de 2022, elevou o patamar normativo da LGPD ao conferir status de direito fundamental explícito à proteção de dados pessoais no ordenamento jurídico brasileiro (BRASIL, 2022). Para os bancos digitais, essa mudança constitucional tem implicações práticas relevantes: a violação de dados pessoais de clientes bancários passa a ser avaliada não apenas sob a ótica das sanções administrativas da LGPD e das penalidades prudenciais do BCB, mas também sob o prisma da responsabilidade civil constitucional, com potencial para ações coletivas de tutela dos direitos fundamentais dos titulares de dados.

A sobreposição de jurisdições regulatórias entre a ANPD e o Banco Central do Brasil representa uma das principais complexidades do cenário de conformidade para os bancos digitais. Enquanto a ANPD tem competência geral para fiscalizar o tratamento de dados pessoais nos termos da LGPD, o BCB exerce supervisão prudencial sobre a gestão de riscos cibernéticos das instituições financeiras. Motta e Rosa (2022) identificam que essa dualidade regulatória é especialmente pronunciada no contexto do open banking e do open finance, em que o compartilhamento de dados financeiros entre múltiplas instituições amplia exponencialmente o perímetro de responsabilidade de cada agente de tratamento. A ausência de um protocolo formal

de coordenação entre os dois reguladores gera incerteza jurídica e custos regulatórios adicionais para as instituições que precisam atender simultaneamente às duas esferas normativas.

A regulação mais recente do BCB aprofunda as exigências de cibersegurança para o setor. As Resoluções CMN n. 538/2025 e BCB n. 538/2025, publicadas em dezembro de 2025 e em vigor a partir de março de 2026, introduziram 14 controles mínimos mandatórios de cibersegurança para fintechs, instituições de pagamento e demais entidades do Sistema Financeiro Nacional, incluindo autenticação multifator para acessos administrativos, isolamento físico e lógico de ambientes críticos em nuvem e validação de integridade de ponta a ponta antes da assinatura digital (Brasil, 2025). Esse avanço regulatório representa uma densificação normativa que eleva o padrão mínimo exigido de todas as instituições financeiras, independentemente do porte, e cria novos parâmetros para a avaliação da conformidade em matéria de cibersegurança.

A Resolução CMN n. 4.893/2021, ao disciplinar a contratação de serviços em nuvem, inaugurou no ordenamento regulatório brasileiro uma abordagem centrada na responsabilidade da instituição financeira pela cadeia de terceiros que integra sua operação digital. Sobre essa obrigação extensível, o próprio texto normativo estabelece:

> As instituições referidas no art. 1º devem assegurar que seus prestadores de serviços relevantes, estabelecidos no País ou no exterior, adotem práticas de segurança cibernética compatíveis com as exigidas da própria instituição. [...] A contratação de serviços de computação em nuvem para processamento, armazenamento de dados ou execução de funções relevantes fica condicionada à comunicação prévia ao Banco Central do Brasil. (Brasil, 2021a)

Esse dispositivo evidencia que a responsabilidade regulatória dos bancos digitais não se encerra em seus próprios sistemas: ela se estende a toda a cadeia de provedores que sustenta sua operação. Trata-se de uma opção normativa alinhada às melhores práticas internacionais de gestão de risco de terceiros recomendadas pelo Comitê de Supervisão Bancária de Basileia, que reconhece a inviabilidade de avaliar a resiliência de uma instituição financeira sem considerar a vulnerabilidade de seus fornecedores tecnológicos críticos.

2.2 Vetores de risco cibernético nos bancos digitais: Tipologia e características

A literatura especializada e os relatórios setoriais convergem na identificação de um conjunto de vetores de risco cibernético predominantes nos bancos digitais. O primeiro e mais crítico desses vetores é o risco de engenharia social, que envolve a manipulação psicológica de usuários e colaboradores para a obtenção de credenciais de acesso, informações confidenciais ou autorização de transações fraudulentas. No contexto dos bancos digitais, esse vetor se manifesta principalmente por meio de ataques de phishing, smishing (via SMS) e vishing (via chamada telefônica), que exploram a familiaridade dos clientes com as interfaces digitais e a ausência de verificação presencial que caracteriza as interações bancárias digitais (NIC.br, 2020). O NIC.br (2020) identificou que a maioria das organizações brasileiras ainda apresenta maturidade insuficiente nas práticas de conscientização e treinamento de usuários para o reconhecimento de tentativas de engenharia social.

O segundo vetor crítico é o risco de terceiros, que decorre da dependência estrutural dos bancos digitais em relação a provedores de computação em nuvem, processadores de pagamentos, parceiros de tecnologia e integradores de API no contexto do open banking. Silva, Garcia Junior e Araújo (2022) observam que o modelo de negócio das fintechs e bancos digitais é, por natureza, altamente integrado a ecossistemas de parceiros tecnológicos, o que cria uma cadeia de dependências que amplia o perímetro de risco de cada instituição bem além de seus próprios sistemas. A Resolução CMN n. 4.893/2021 reconhece explicitamente esse vetor ao disciplinar a contratação de serviços em nuvem e ao exigir a devida diligência cibernética dos provedores, mas sua efetividade depende da capacidade das instituições de monitorar continuamente uma cadeia de terceiros cada vez mais extensa e dinâmica (Brasil, 2021a).

O FMI (2020) alerta que a concentração de serviços de processamento e armazenamento em poucos provedores globais de computação em nuvem cria riscos de concentração sistêmica no setor financeiro: uma falha ou um ataque a um desses provedores pode comprometer simultaneamente dezenas de instituições financeiras, gerando efeitos em cascata com potencial para instabilidade sistêmica. Essa preocupação é especialmente relevante para os bancos digitais brasileiros, que em sua maioria operam sobre infraestruturas de nuvem pública de grandes provedores globais. O relatório do FMI destaca que a cooperação internacional entre reguladores e o compartilhamento de informações sobre ameaças são condições necessárias para

a gestão efetiva desse risco de concentração, o que exige iniciativas que transcendem o poder de ação unilateral de qualquer regulador nacional.

A Pesquisa Febraban de Tecnologia Bancária (Febraban/Deloitte, 2024) documenta que os ataques de ransomware, modalidade em que sistemas são sequestrados por criminosos que exigem pagamento para a restituição do acesso, tornaram-se um dos vetores mais frequentes e danosos para o setor financeiro brasileiro. Esse tipo de ataque explora vulnerabilidades na segurança de redes, brechas em sistemas de autenticação e a ausência de segmentação de ambientes críticos, comprometendo tanto a disponibilidade dos serviços quanto a integridade dos dados. Para os bancos digitais, a indisponibilidade de sistemas, mesmo por poucas horas, pode gerar danos reputacionais severos e perda irreversível de confiança dos clientes.

O terceiro vetor de risco identificado na literatura é o risco de identidade e autenticação, que envolve o comprometimento de credenciais de acesso de clientes e colaboradores por meio de ataques de força bruta, preenchimento de credenciais (credential stuffing) e exploração de vazamentos de dados em outras plataformas. Doneda (2020) ressalta que a proteção de dados pessoais no setor financeiro deve incorporar mecanismos de autenticação robustos como elemento central da arquitetura de segurança, pois os dados bancários são extremamente valiosos para a execução de fraudes financeiras. O princípio da segurança, previsto no artigo 6º, VII, da LGPD (Brasil, 2018), exige que as instituições adotem medidas técnicas aptas a prevenir o acesso não autorizado a dados pessoais, o que, no contexto bancário digital, se traduz na implementação obrigatória de autenticação multifator, monitoramento de sessões e detecção de anomalias comportamentais.

A Pesquisa Febraban de Tecnologia Bancária (Febraban/Deloitte, 2023) registra que, entre as prioridades dos bancos para a área de segurança cibernética, figuram a cibersegurança inteligente, baseada em múltiplos métodos de verificação e autenticação, e a resposta a incidentes em tempo real. Sobre o papel da inteligência artificial nesse contexto, o relatório afirma:

> A adoção de inteligência artificial para detecção de fraudes e anomalias em tempo real representa um avanço significativo nas estratégias de defesa ativa dos bancos. Contudo, a efetividade dessas tecnologias depende da qualidade dos dados de treinamento dos algoritmos e da existência de equipes

> especializadas capazes de interpretar os alertas gerados e tomar decisões ágeis de contenção. (Febraban/Deloitte, 2023)

Esse ponto revela uma tensão estrutural que percorre todo o setor: os bancos investem crescentemente em automação da segurança, mas a interpretação qualificada dos alertas gerados pelos sistemas continua sendo uma atribuição humana insubstituível. O deficit de profissionais especializados em cibersegurança, documentado nos relatórios mais recentes, coloca em risco a própria efetividade dos investimentos tecnológicos realizados pelas instituições financeiras digitais.

Por fim, o risco regulatório e de conformidade constitui um vetor indireto, mas relevante, de vulnerabilidade para os bancos digitais. A necessidade de atender simultaneamente às exigências da LGPD, da Resolução CMN n. 4.893/2021 e de outras normas setoriais, como as regras do open finance e as resoluções mais recentes sobre controles mínimos de cibersegurança, impõe às instituições uma carga de conformidade que, se não for adequadamente gerenciada, pode resultar em sobreposições, lacunas e incoerências nos controles implementados. Motta e Rosa (2022) identificam que a fragmentação normativa é um dos principais fatores que dificultam a implementação de uma arquitetura de segurança coerente e eficaz nos bancos digitais, especialmente naqueles de menor porte que não dispõem de equipes jurídicas e técnicas suficientes para gerenciar a complexidade do ambiente regulatório.

2.3 Governança de resposta a incidentes: Modelos, práticas e desafios

A governança de resposta a incidentes cibernéticos compreende o conjunto de políticas, processos, papéis e responsabilidades que orientam as ações de uma organização diante da ocorrência de um incidente de segurança. Para os bancos digitais, essa governança assume caráter crítico, pois a velocidade e a qualidade da resposta a um incidente determinam a extensão dos danos sofridos pelos clientes, pela própria instituição e pelo sistema financeiro como um todo. A Resolução CMN n. 4.893/2021 disciplina explicitamente a obrigação de elaboração de um plano de ação e resposta a incidentes que contemple os procedimentos de contenção, erradicação, recuperação e comunicação, tanto interna quanto aos reguladores e aos clientes afetados (Brasil, 2021a). Esse plano deve ser testado periodicamente e ajustado com base nos resultados dos testes de continuidade de negócios.

Bioni (2021) observa que a obrigação de comunicação de incidentes prevista na LGPD representa uma mudança cultural significativa para as organizações brasileiras, que historicamente tendiam a manter sigilo sobre vazamentos de dados por receio de danos reputacionais. A lógica subjacente ao artigo 48 da LGPD (BRASIL, 2018) é inversa: a comunicação tempestiva e transparente de incidentes permite que os titulares adotem medidas de autoproteção, que os reguladores avaliem a extensão do dano e que o mercado sinalize às instituições que a responsabilidade pela segurança dos dados é um elemento central de sua proposta de valor para os clientes. Para os bancos digitais, cuja relação com os clientes é exclusivamente digital e fortemente mediada pela confiança na segurança da plataforma, a transparência na gestão de incidentes é um requisito de sobrevivência competitiva.

Os modelos de resposta a incidentes mais adotados internacionalmente, como o framework NIST (National Institute of Standards and Technology) e o padrão ISO/IEC 27035, estruturam o ciclo de resposta em cinco fases: preparação, identificação, contenção, erradicação e recuperação, seguidas de uma fase de lições aprendidas. No contexto regulatório brasileiro, a Resolução CMN n. 4.893/2021 incorpora implicitamente essa estrutura ao exigir que as instituições definam procedimentos para cada uma dessas etapas, embora não faça referência explícita a nenhum framework específico, deixando às próprias instituições a escolha das metodologias a adotar. Silva, Garcia Junior e Araújo (2022) observam que a flexibilidade regulatória, embora seja um acerto do ponto de vista da adaptabilidade às especificidades de cada instituição, pode gerar inconsistências nas práticas de resposta a incidentes, especialmente quando o incidente envolve múltiplas instituições interconectadas pelo ecossistema do open finance.

A Febraban e a Deloitte registram, nas edições mais recentes da Pesquisa de Tecnologia Bancária, que os bancos brasileiros avançaram significativamente na adoção de Centros de Operações de Segurança (SOC), que funcionam como estruturas permanentes de monitoramento e resposta a ameaças em tempo real. Entretanto, o mesmo estudo indica que 79% das instituições financeiras identificam o acesso a profissionais qualificados como um dos principais desafios da gestão de cibersegurança, evidenciando que o investimento em tecnologia não é acompanhado pelo desenvolvimento proporcional do capital humano especializado (Febraban/Deloitte, 2024). Esse desequilíbrio compromete a efetividade dos SOCs e

cria dependência excessiva de ferramentas automatizadas, que, embora úteis, não substituem a capacidade analítica de profissionais experientes na interpretação e no tratamento de incidentes complexos.

A complexidade da governança de resposta a incidentes nos bancos digitais é ampliada pela necessidade de coordenar ações com múltiplos reguladores em caso de incidentes que envolvam simultaneamente dados pessoais e infraestrutura crítica. Nesses casos, a instituição deve notificar tanto a ANPD, nos termos do artigo 48 da LGPD, quanto o Banco Central do Brasil, nos termos da Resolução CMN n. 4.893/2021, em prazos e formatos que podem diferir entre si. Doneda (2020) destaca que a efetividade do regime de proteção de dados depende, em última instância, da capacidade institucional dos órgãos reguladores de processar e responder às notificações de incidentes de forma ágil e coordenada, o que exige não apenas recursos humanos e tecnológicos adequados, mas também mecanismos formais de cooperação interinstitucional ainda em construção no Brasil.

A dimensão da resposta a incidentes ligada à comunicação com os clientes afetados merece atenção especial no contexto dos bancos digitais. Diferentemente dos bancos tradicionais, que dispõem de redes de agências para comunicações presenciais, os bancos digitais dependem exclusivamente de canais digitais (aplicativos, e-mail, SMS) para informar seus clientes sobre incidentes e as medidas de proteção recomendadas. Isso cria um paradoxo: os mesmos canais que podem ter sido comprometidos no incidente são aqueles pelos quais a instituição precisa comunicar o ocorrido. A elaboração de planos de comunicação de crise que contemplem canais alternativos e mensagens pré-aprovadas de comunicação a clientes é, portanto, uma exigência prática da governança de resposta a incidentes que vai além do texto da Resolução CMN n. 4.893/2021, mas que está implícita em suas obrigações de continuidade de negócios (Brasil, 2021a).

3 METODOLOGIA

A presente pesquisa adota a abordagem qualitativa de natureza bibliográfica e documental, caracterizada pela análise crítica e interpretativa de fontes secundárias: legislação, normativas regulatórias, literatura científica e relatórios técnicos de organizações nacionais e internacionais, sem a realização de coleta de dados primários junto a indivíduos ou organizações. Essa escolha metodológica é adequada

ao objetivo do estudo, que consiste em analisar e sintetizar o estado do conhecimento sobre cibersegurança e proteção de dados nos bancos digitais brasileiros a partir das fontes disponíveis na literatura especializada e no ordenamento jurídico vigente. A abordagem qualitativa permite capturar a complexidade das relações entre as dimensões jurídica, técnica e organizacional do problema, que não seriam adequadamente tratadas por metodologias quantitativas.

O levantamento das fontes foi realizado nas seguintes bases de dados e repositórios: Portal de Periódicos da CAPES; Scientific Electronic Library Online (SciELO); Google Scholar; repositório da Revista da Procuradoria-Geral do Banco Central (Revista PGBC), disponível em revistapgbc.bcb.gov.br; Portal de Legislação do Governo Federal, disponível em planalto.gov.br; Portal do Banco Central do Brasil, disponível em bcb.gov.br; repositório do NIC.br/CETIC.br; e portal da FEBRABAN. As buscas foram conduzidas com os seguintes descritores, em português e inglês, utilizados de forma isolada e combinada: 'cibersegurança', 'segurança cibernética', 'bancos digitais', 'fintechs', 'LGPD', 'proteção de dados', 'resposta a incidentes', 'Resolução 4.893', 'open banking' e 'sistema financeiro'. O recorte temporal prioritário das publicações abrange o período de 2018 a 2025, com inclusão de obras anteriores de relevância teórica incontornável.

Os critérios de inclusão das fontes foram: (i) pertinência temática direta ao objeto de estudo; (ii) disponibilidade em acesso aberto ou em bases de dados acadêmicas verificáveis; (iii) autoria identificada e afiliação institucional ou editorial comprovável; (iv) publicação em periódico arbitrado, obra acadêmica reconhecida, por órgão público ou organização internacional de reconhecida credibilidade. Os critérios de exclusão compreenderam: materiais sem autoria identificada, publicações de natureza exclusivamente comercial sem embasamento acadêmico e obras cujos dados bibliográficos não foram passíveis de verificação nas bases consultadas

A análise documental compreendeu o estudo sistemático da legislação federal pertinente, notadamente a Lei n. 13.709/2018, a Emenda Constitucional n. 115/2022 e a Resolução CMN n. 4.893/2021, bem como dos relatórios técnicos das organizações consultadas, com especial atenção às edições de 2023 e 2024 da Pesquisa Febraban de Tecnologia Bancária, que documentam empiricamente o estado dos investimentos e das prioridades em segurança cibernética no setor

bancário brasileiro. A análise normativa seguiu os cânones da interpretação jurídica sistemática e teleológica, buscando identificar a coerência e as eventuais lacunas entre os diferentes instrumentos regulatórios que incidem sobre os bancos digitais.

A síntese dos resultados foi conduzida pelo método de análise de conteúdo qualitativa, que permitiu agrupar os achados das fontes consultadas em categorias temáticas correspondentes aos objetivos específicos da pesquisa. As quatro categorias analíticas identificadas foram: (a) arcabouço regulatório e sua efetividade; (b) tipologia dos vetores de risco cibernético nos bancos digitais; (c) estratégias de prevenção e resposta a incidentes; e (d) desafios de conformidade simultânea com a LGPD e com a regulação prudencial do BCB. A principal limitação metodológica consiste na ausência de dados primários coletados junto a gestores de bancos digitais, o que restringe as conclusões ao plano da análise normativa e da literatura disponível, sem contemplar a perspectiva dos profissionais que atuam operacionalmente nos processos de conformidade e resposta a incidentes.

A integridade científica da pesquisa foi assegurada pela adoção rigorosa dos critérios de inclusão e exclusão de fontes, pela verificação da existência e acessibilidade de todos os documentos citados e pela vedação ao uso de qualquer referência não verificável nas bases consultadas. Nenhum autor, obra, editora ou dado foi inventado ou inferido sem fundamento nas fontes primárias. Todas as referências bibliográficas constam devidamente identificadas na seção final do artigo, com dados completos de publicação e, quando disponível, o endereço eletrônico para acesso.

4 RESULTADOS E DISCUSSÃO

A análise das fontes consultadas permite identificar um primeiro resultado de destaque: o Brasil construiu, ao longo dos últimos anos, um dos arcabouços regulatórios de cibersegurança mais abrangentes da América Latina para o setor financeiro, com a conjugação da LGPD e da Resolução CMN n. 4.893/2021. Contudo, a mera existência do marco normativo não garante a efetividade da proteção. A Pesquisa Febraban de Tecnologia Bancária (Febraban/Deloitte, 2024) documenta que, embora 100% dos bancos entrevistados declarem a cibersegurança como prioridade estratégica, apenas uma parcela deles demonstra maturidade operacional plena nos indicadores de governança cibernética, resposta a incidentes e gestão de risco de terceiros. Esse hiato entre a prioridade declarada e a maturidade efetiva

constitui o primeiro achado relevante desta pesquisa, sinalizando que os investimentos crescentes em tecnologia precisam ser acompanhados de avanços equivalentes em governança e capital humano.

O segundo resultado relevante refere-se à assimetria de maturidade entre bancos digitais de grande porte e fintechs menores. Silva, Garcia Junior e Araújo (2022) documentam que os bancos digitais de grande escala, como Nubank, Banco Inter e C6 Bank, dispõem de recursos humanos e tecnológicos muito superiores aos de fintechs em estágio inicial, embora todos estejam sujeitos às mesmas obrigações regulatórias da Resolução CMN n. 4.893/2021. Essa assimetria cria uma vulnerabilidade sistêmica: as fintechs menores, que também integram o ecossistema do open finance e processam dados pessoais de milhares de clientes, podem tornar-se pontos de entrada para ataques que, a partir delas, alcançam instituições de maior porte na cadeia de integração. O regulador reconhece essa assimetria ao adotar uma abordagem proporcional, mas a proporcionalidade não pode implicar tolerância com controles mínimos abaixo do patamar necessário para a proteção efetiva dos clientes.

O terceiro achado da pesquisa diz respeito à centralidade do risco de terceiros como vetor de ataque nos bancos digitais. A dependência estrutural dessas instituições em relação a provedores de computação em nuvem e integradores de API, documentada por Motta e Rosa (2022) no contexto do open banking, cria uma superfície de ataque que transcende o perímetro de controle de cada banco digital individualmente. O FMI (2020) alertou que a concentração de serviços em poucos provedores globais de nuvem amplifica esse risco ao nível sistêmico, pois uma falha em um provedor pode comprometer simultaneamente múltiplas instituições financeiras. A Resolução CMN n. 4.893/2021 endereça esse risco ao exigir avaliação e monitoramento dos provedores, mas a efetividade dessa exigência depende da capacidade operacional das equipes de compliance, frequentemente insuficiente para o tamanho e a dinamicidade da cadeia de fornecedores dos bancos digitais (Brasil, 2021a).

Em relação às estratégias de prevenção, os resultados evidenciam que os bancos digitais brasileiros avançaram de forma consistente na adoção de tecnologias de detecção e resposta em tempo real, especialmente na integração de inteligência artificial para identificação de fraudes e anomalias comportamentais. A Pesquisa

Febraban (Febraban/Deloitte, 2023) registra que a cibersegurança inteligente, baseada em múltiplos métodos de verificação e autenticação, tornou-se a principal diretriz tecnológica do setor para a prevenção de incidentes. Entretanto, a dimensão humana da prevenção, que abrange a conscientização de clientes e colaboradores, o treinamento para reconhecimento de engenharia social e a construção de uma cultura de segurança, ainda recebe investimentos desproporcionalmente menores em relação às soluções tecnológicas. O NIC.br (2020) registra que a maioria das organizações brasileiras ainda apresenta lacunas significativas nas práticas de treinamento e conscientização, o que é especialmente preocupante para os bancos digitais, cujos canais de atendimento digital são os principais vetores de ataques de phishing e engenharia social dirigidos aos clientes.

O quinto resultado relevante refere-se à governança de resposta a incidentes. A análise da Resolução CMN n. 4.893/2021 (Brasil, 2021a) e da LGPD (Brasil, 2018) evidencia que ambas as normas exigem a existência de planos de resposta a incidentes e a comunicação tempestiva de incidentes relevantes aos reguladores e, no caso da LGPD, também aos titulares afetados. Bioni (2021) observa que a obrigação de comunicação da LGPD representa uma ruptura com a cultura de sigilo sobre incidentes que historicamente prevaleceu no setor, criando um incentivo institucional à transparência. Na prática, contudo, a sobreposição de obrigações de reporte a dois reguladores distintos (ANPD e BCB) sem um protocolo unificado de comunicação gera inconsistências e custos regulatórios que podem retardar a resposta institucional justamente no momento em que a agilidade é mais crítica.

Por fim, os resultados indicam que a constitucionalização da proteção de dados, operada pela EC n. 115/2022 (Brasil, 2022), tem potencial para transformar o regime de responsabilidade civil dos bancos digitais por incidentes de segurança que envolvam dados pessoais de clientes. Ao elevar a proteção de dados ao patamar de direito fundamental, a Emenda abre espaço para ações coletivas de tutela constitucional, com potencial de indenizações de natureza preventiva e punitiva que vão muito além das sanções administrativas da LGPD. Doneda (2020) antecipou esse cenário ao argumentar que a proteção de dados, enquanto manifestação do direito à privacidade e à autodeterminação informacional, tem fundamento constitucional mesmo antes da EC n. 115/2022. Esse cenário jurídico emergente deverá induzir os bancos digitais a intensificar seus investimentos em prevenção e governança, pois o

custo potencial de uma violação de dados vai muito além das sanções administrativas formalmente previstas.

5 CONSIDERAÇÕES FINAIS

O presente estudo analisou as estratégias de prevenção e resposta a incidentes cibernéticos nos bancos digitais brasileiros, investigando a articulação entre as exigências da LGPD e os requisitos de segurança cibernética estabelecidos pela Resolução CMN n. 4.893/2021. O objetivo geral da pesquisa foi alcançado: a análise demonstrou que o Brasil dispõe de um arcabouço regulatório abrangente e bem articulado para a gestão de riscos cibernéticos no setor financeiro digital, mas que a efetividade desse marco normativo é comprometida por lacunas de maturidade operacional, assimetria entre instituições de diferentes portes e ausência de coordenação interinstitucional entre os reguladores.

O primeiro objetivo específico, consistente em caracterizar o marco regulatório de cibersegurança aplicável aos bancos digitais, foi plenamente atingido. A análise evidenciou que a conjugação da LGPD, da Resolução CMN n. 4.893/2021, da Emenda Constitucional n. 115/2022 e das normativas mais recentes do BCB cria uma estrutura normativa de múltiplas camadas que impõe aos bancos digitais obrigações técnicas e jurídicas simultâneas e complementares. A recente densificação normativa, com a introdução dos 14 controles mínimos mandatórios de cibersegurança a partir de 2026, representa um avanço regulatório significativo que eleva o padrão mínimo exigido de todas as instituições do Sistema Financeiro Nacional.

O segundo objetivo específico, relativo à identificação dos principais vetores de ataque e das estratégias de prevenção adotadas, foi igualmente alcançado. Os vetores de risco mais críticos identificados são: engenharia social dirigida a clientes e colaboradores; risco de terceiros decorrente da dependência de provedores de nuvem e parceiros de tecnologia; ataques de ransomware explorando vulnerabilidades em redes e sistemas; risco de identidade por comprometimento de credenciais; e risco regulatório e de conformidade decorrente da fragmentação normativa. As estratégias de prevenção mais efetivas envolvem a combinação de tecnologias de detecção em tempo real baseadas em inteligência artificial, autenticação multifator, segmentação de ambientes críticos e conscientização contínua de usuários.

O terceiro objetivo específico, que consistia em analisar os desafios de conformidade simultânea com a LGPD e com a regulação do BCB, revelou que a ausência de um protocolo formal de coordenação entre a ANPD e o Banco Central representa a principal lacuna institucional do arcabouço regulatório vigente. A sobreposição de jurisdições e a falta de mecanismos de compartilhamento de informações entre os dois reguladores impõem custos adicionais às instituições e podem retardar a resposta a incidentes graves que envolvam simultaneamente dados pessoais e infraestrutura crítica do sistema financeiro.

Do ponto de vista das implicações práticas para os bancos digitais, a pesquisa evidencia a necessidade urgente de integração entre as áreas de cibersegurança, compliance, jurídico e tecnologia da informação. Essa integração é indispensável para que as instituições consigam gerir de forma coerente e eficiente as múltiplas obrigações regulatórias a que estão sujeitas, evitando sobreposições e lacunas nos controles implementados. A criação de comitês interfuncionais de governança cibernética, com participação da alta administração e reporte periódico ao conselho de administração, representa uma boa prática recomendada tanto pela Resolução CMN n. 4.893/2021 quanto pelos princípios de responsabilização e prestação de contas da LGPD.

No plano das políticas públicas, o estudo recomenda a elaboração de um protocolo formal de cooperação entre a ANPD e o Banco Central do Brasil, que estabeleça mecanismos claros de compartilhamento de informações sobre incidentes e de harmonização dos requisitos de reporte, com vistas a reduzir a carga regulatória sobre as instituições e ampliar a efetividade da supervisão. Recomenda-se, ainda, que as normativas mais recentes sobre controles mínimos de cibersegurança sejam acompanhadas de programas de capacitação técnica para as instituições de menor porte, que carecem de recursos para sua plena implementação.

A pesquisa aponta, adicionalmente, para a necessidade de investimento público e privado em formação de profissionais de cibersegurança especializados no setor financeiro. O déficit de talentos identificado pela Pesquisa FEBRABAN de Tecnologia Bancária é uma das principais restrições à efetividade das políticas de cibersegurança no Brasil e constitui um problema que não pode ser resolvido apenas

por meio de mais regulação, exigindo iniciativas de educação, certificação e atração de carreiras na área de segurança da informação.

A dimensão humana da cibersegurança, que compreende a conscientização de clientes, o treinamento de colaboradores e a construção de uma cultura organizacional de segurança, emerge da análise como um vetor de investimento subvalorizado em relação ao volume de recursos destinado às soluções tecnológicas. A efetividade das melhores tecnologias de segurança depende, em última instância, de pessoas bem treinadas e de uma cultura organizacional que trate a segurança cibernética como responsabilidade coletiva e não como atribuição exclusiva das equipes de tecnologia da informação. Os bancos digitais, por sua natureza totalmente digital e pela intensidade do contato com clientes por meio de plataformas móveis, têm uma responsabilidade especial na educação de seus usuários sobre práticas seguras de navegação e autenticação.

A constitucionalização da proteção de dados pessoais pela Emenda Constitucional n. 115/2022 representa um divisor de águas no regime de responsabilidade dos bancos digitais por incidentes de segurança. O potencial para ações coletivas de tutela constitucional, com indenizações de natureza preventiva e punitiva, cria um incentivo econômico poderoso para que as instituições antecipem investimentos em prevenção, em vez de aguardar a ocorrência de incidentes para tomar medidas corretivas. Essa lógica de prevenção ativa deve orientar as estratégias de governança de risco cibernético dos bancos digitais nos próximos anos.

Entre as limitações desta pesquisa, destaca-se a ausência de dados primários coletados junto a gestores e equipes de compliance dos bancos digitais, o que circunscreveu as conclusões ao plano da análise normativa e da literatura disponível. Pesquisas futuras que combinem a revisão bibliográfica com estudos de caso aprofundados em bancos digitais específicos, entrevistas com profissionais de cibersegurança e compliance e análise comparada com outros sistemas financeiros digitais poderão aprofundar os diagnósticos aqui apresentados e validar empiricamente as recomendações formuladas.

Em síntese, a cibersegurança e a proteção de dados no setor de bancos digitais brasileiro demandam não apenas um marco regulatório robusto, que o Brasil já possui em grande medida, mas também uma mudança cultural profunda nas

organizações, que incorpore a segurança como valor estratégico e não como mera obrigação de conformidade. Os bancos digitais que construírem essa cultura organizacional de segurança, investindo simultaneamente em tecnologia, governança e capital humano, estarão melhor posicionados para proteger seus clientes, atender às exigências regulatórias e competir com vantagem em um mercado financeiro digital cada vez mais exigente e suscetível a ameaças cibernéticas sofisticadas.

6 REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. ISBN 9788530994082.

BRASIL. Constituição da República Federativa do Brasil de 1988. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Senado Federal, 2022. Disponível em: https://www.planalto.gov.br. Acesso em: mar. 2025.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: mar. 2025.

BRASIL. Banco Central do Brasil. Resolução CMN n. 4.893, de 26 de fevereiro de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília: BCB, 2021a. Disponível em: https://www.bcb.gov.br. Acesso em: mar. 2025.

BRASIL. Banco Central do Brasil. Resolução BCB n. 85, de 8 de abril de 2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem pelas instituições de pagamento. Brasília: BCB, 2021b. Disponível em: https://www.bcb.gov.br. Acesso em: mar. 2025.

BRASIL. Banco Central do Brasil. Resoluções CMN n. 538 e BCB n. 538, de 18 de dezembro de 2025. Introduzem controles mínimos de cibersegurança para instituições

do Sistema Financeiro Nacional. Brasília: BCB, 2025. Disponível em: https://www.bcb.gov.br. Acesso em: mar. 2026.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2020.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN); DELOITTE. Pesquisa FEBRABAN de Tecnologia Bancária 2023. São Paulo: FEBRABAN/Deloitte, 2023. Disponível em: https://portal.febraban.org.br/pagina/3106/1117/pt-br/pesquisa. Acesso em: mar. 2025.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN); DELOITTE. Pesquisa FEBRABAN de Tecnologia Bancária 2024. São Paulo: FEBRABAN/Deloitte, 2024. Disponível em: https://portal.febraban.org.br/noticia/4091/pt-br/. Acesso em: mar. 2025.

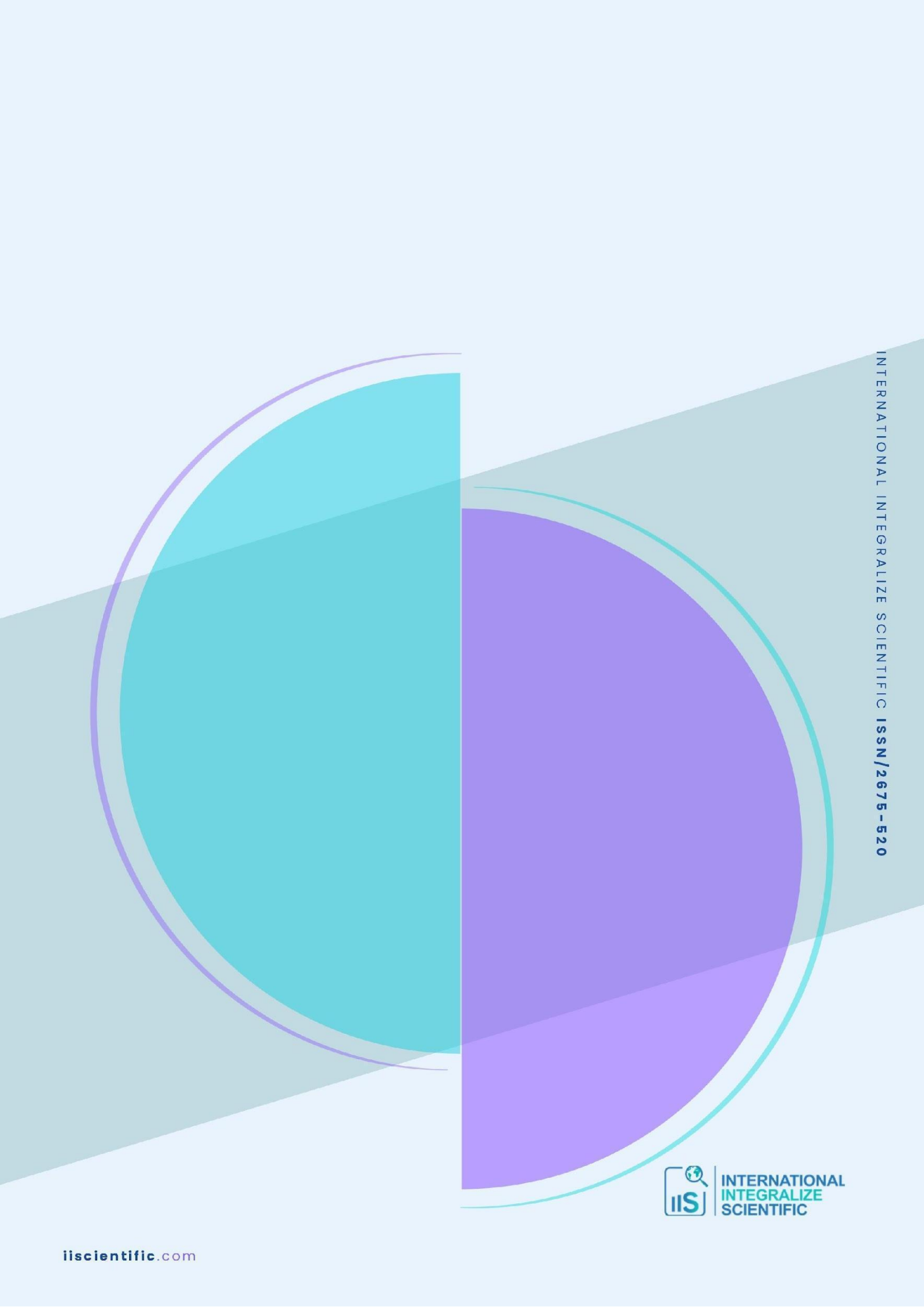
FUNDO MONETÁRIO INTERNACIONAL (FMI). O risco cibernético é a nova ameaça à estabilidade financeira. Blog do FMI, 7 dez. 2020. Disponível em: https://www.imf.org/pt/blogs/articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability. Acesso em: mar. 2025.

MOTTA, Bernardo Rocha da; ROSA, Marcus Paulus de Oliveira. Open Banking, Big Data e Inteligência Artificial: como tudo está conectado na regulação de um sistema financeiro e de pagamentos movido a dados? Revista da Procuradoria-Geral do Banco Central, Brasília, v. 16, n. 1, p. 132-154, jun. 2022. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1163. Acesso em: mar. 2025.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Segurança digital: uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf. Acesso em: mar. 2025.

SILVA, Vitória Batista Santos; GARCIA JUNIOR, Wagner Roberto Ramos; ARAÚJO, Clayton Vinicius Pegoraro de. Fintechs: (r)evolução bancária na era da economia digital. Revista da Procuradoria-Geral do Banco Central, Brasília, v. 16, n. 1, p. 65-77, jun. 2022. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1155/79. Acesso em: mar. 2025.

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520



INTERNATIONAL INTEGRALIZE SCIENTIFIC