INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Abril 2026

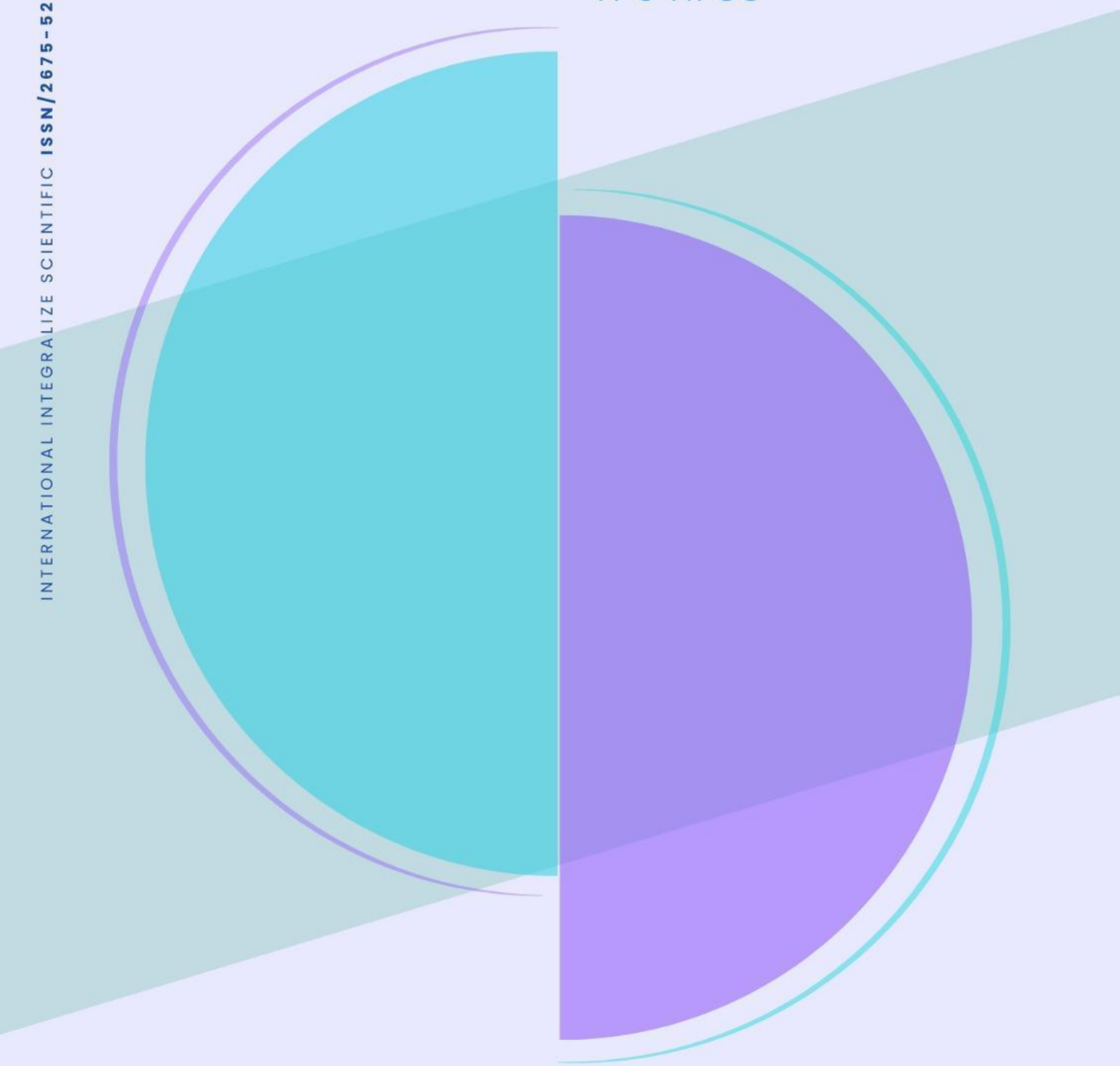
v. 6 n. 58

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

GESTÃO DE RISCOS DE DADOS SENSÍVEIS EM INSTITUIÇÕES FINANCEIRAS BRASILEIRAS: DESAFIOS REGULATÓRIOS E TECNOLÓGICOS NA ERA DO OPEN FINANCE

MANAGEMENT OF SENSITIVE DATA RISKS IN BRAZILIAN FINANCIAL INSTITUTIONS: REGULATORY AND TECHNOLOGICAL CHALLENGES IN THE OPEN FINANCE ERA

GESTIÓN DE RIESGOS DE DATOS SENSIBLES EN INSTITUCIONES FINANCIERAS BRASILEÑAS: DESAFÍOS REGULATORIOS Y TECNOLÓGICOS EN LA ERA DEL OPEN FINANCE

RESUMO

O artigo investiga os desafios regulatórios e tecnológicos da gestão de riscos de dados sensíveis em instituições financeiras brasileiras no contexto do open finance. O estudo parte da constatação de que a expansão do sistema financeiro aberto ampliou exponencialmente a circulação de dados pessoais e financeiros entre instituições participantes, tornando a proteção dessas informações uma questão central tanto para o compliance jurídico quanto para a sustentabilidade operacional do setor. Examina-se de que maneira o marco regulatório vigente, composto essencialmente pela Lei Geral de Proteção de Dados Pessoais e pelas normativas do Banco Central do Brasil, estrutura as obrigações das instituições financeiras no tratamento e na segurança de dados sensíveis. A pesquisa adota a metodologia bibliográfica e documental de natureza qualitativa, com análise crítica de legislação federal, normativas setoriais, literatura científica indexada em bases acadêmicas e relatórios técnicos de organismos nacionais e internacionais de reconhecida credibilidade. Os resultados evidenciam que, embora o Brasil disponha de um arcabouço normativo inovador e internacionalmente referenciado, a efetividade da proteção de dados no ambiente do open finance é comprometida por lacunas de coordenação interinstitucional, assimetrias tecnológicas entre os agentes participantes e insuficiência de mecanismos de gestão de risco de terceiros. Constata-se, adicionalmente, que a dimensão humana da segurança, traduzida em cultura organizacional de proteção de dados e capacitação de equipes, permanece subvalorizada em relação aos investimentos em soluções tecnológicas. O estudo contribui para o debate acadêmico e institucional sobre a governança de dados sensíveis no sistema financeiro e aponta caminhos para o aprimoramento das políticas regulatórias voltadas à proteção da privacidade dos usuários na economia digital.

Palavras-chave: Open finance; dados sensíveis; LGPD; gestão de riscos; instituições financeiras.

ABSTRACT

This article investigates the regulatory and technological challenges of sensitive data risk management in Brazilian financial institutions in the context of open finance. The study starts from the observation that the expansion of the open financial system exponentially increased the circulation of personal and financial data among participating institutions, making the protection of this information a central issue for both legal compliance and the operational sustainability of the sector. It examines how the current regulatory framework, essentially composed of the General Personal Data Protection Law and the standards of the Central Bank of Brazil, structures the obligations of financial institutions in the handling and security of sensitive data. The research adopts a qualitative bibliographic and documentary methodology, with critical analysis of federal legislation, sectoral regulations, scientific literature indexed in academic databases and technical reports from nationally and internationally recognized organizations. The results show that, although Brazil has an innovative and internationally referenced regulatory framework, the effectiveness of data protection in the open finance environment is undermined by gaps in interinstitutional coordination, technological asymmetries among participating agents, and insufficient third-party risk management mechanisms. It is also noted that the human dimension of security, translated into an organizational culture of data protection and team training, remains undervalued in relation to investments in technological solutions. The study contributes to the

academic and institutional debate on sensitive data governance in the financial system and points to ways for improving regulatory policies aimed at protecting users' privacy in the digital economy.
Keywords: Open finance; sensitive data; LGPD; risk management; financial institutions.

RESUMEN

El presente artículo investiga los desafíos regulatorios y tecnológicos de la gestión de riesgos de datos sensibles en instituciones financieras brasileñas en el contexto del open finance. El estudio parte de la constatación de que la expansión del sistema financiero abierto amplió exponencialmente la circulación de datos personales y financieros entre instituciones participantes, convirtiendo la protección de esta información en una cuestión central tanto para el cumplimiento jurídico como para la sostenibilidad operacional del sector. Se examina de qué manera el marco regulatorio vigente, compuesto esencialmente por la Ley General de Protección de Datos Personales y las normativas del Banco Central de Brasil, estructura las obligaciones de las instituciones financieras en el tratamiento y la seguridad de datos sensibles. La investigación adopta la metodología bibliográfica y documental de naturaleza cualitativa, con análisis crítico de legislación federal, normativas sectoriales, literatura científica indexada en bases académicas e informes técnicos de organismos nacionales e internacionales de reconocida credibilidad. Los resultados evidencian que, aunque Brasil dispone de un marco normativo innovador e internacionalmente referenciado, la efectividad de la protección de datos en el entorno del open finance es comprometida por brechas de coordinación interinstitucional, asimetrías tecnológicas entre los agentes participantes e insuficiencia de mecanismos de gestión de riesgos de terceros. Se constata, adicionalmente, que la dimensión humana de la seguridad, traducida en cultura organizacional de protección de datos y capacitación de equipos, permanece subvalorada en relación con las inversiones en soluciones tecnológicas. El estudio contribuye al debate académico e institucional sobre la gobernanza de datos sensibles en el sistema financiero y apunta caminos para el perfeccionamiento de las políticas regulatorias orientadas a la protección de la privacidad de los usuarios en la economía digital.
Palabras clave: Open finance; datos sensibles; LGPD; gestión de riesgos; instituciones financieras.

1 INTRODUÇÃO

A transformação digital do sistema financeiro brasileiro avançou em ritmo acelerado nos últimos anos, impulsionada pela criação do ecossistema de open finance, que permite o compartilhamento estruturado e padronizado de dados pessoais e financeiros entre instituições participantes autorizadas pelo Banco Central do Brasil. O país se consolidou, rapidamente, como um dos ecossistemas de open finance mais avançados do mundo: segundo dados divulgados pela Associação Open Finance Brasil, o ecossistema já reúne mais de 100 milhões de clientes ou contas conectadas e 154 milhões de consentimentos ativos, com crescimento de 143% no número de consentimentos únicos no biênio 2024-2025 (OpenFinanceBrasil.org.br, 2026). Esse crescimento vertiginoso, embora eloquente quanto à aceitação da iniciativa, impõe uma questão inevitável: como as instituições financeiras estão gerindo os riscos associados ao tráfego massivo de dados sensíveis que sustenta todo esse ecossistema?

A resposta a essa pergunta passa necessariamente pela análise do marco regulatório que disciplina o tratamento de dados pessoais no setor financeiro. A Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709/2018) estabeleceu, no plano normativo geral, os princípios, as bases legais e as obrigações de segurança que governam o tratamento de dados no Brasil, incluindo os dados financeiros. Em paralelo, o Banco Central editou a Resolução CMN n. 4.893/2021, que impôs às instituições autorizadas a estruturação de políticas formais de segurança cibernética, planos de resposta a incidentes e critérios específicos para a contratação de provedores de computação em nuvem. A arquitetura regulatória resultante é densa e, ao mesmo tempo, apresenta lacunas que a literatura especializada tem procurado identificar e debater. Motta e Rosa (2022), em artigo publicado na Revista da Procuradoria-Geral do Banco Central, registram que o open banking, ao expandir de forma estrutural o compartilhamento de dados entre instituições financeiras, levanta questões jurídicas e éticas ainda não plenamente equacionadas pelo ordenamento vigente, especialmente no que se refere ao tratamento algorítmico de dados e à proteção dos titulares contra usos discriminatórios.

Do ponto de vista tecnológico, o open finance opera por meio de interfaces de programação de aplicações (APIs) padronizadas, que permitem a troca automatizada e em tempo real de dados cadastrais, transacionais e de produtos financeiros entre as instituições participantes. Essa arquitetura, embora eficiente do ponto de vista da interoperabilidade, amplia significativamente a superfície de exposição a riscos cibernéticos: cada API representa um ponto de entrada potencial para ataques externos, e a cadeia de integrações entre instituições cria uma rede de dependências cujas vulnerabilidades se propagam de forma sistêmica. Paravela e Domingues (2021), ao analisarem a implementação do open banking na perspectiva do consumidor, alertam que o sistema financeiro aberto intensifica as preocupações com o compartilhamento de dados pessoais sobre serviços bancários e exige uma interação mais coordenada entre os órgãos competentes, especialmente entre o Banco Central do Brasil e a Autoridade Nacional de Proteção de Dados (ANPD).

A justificativa para o presente estudo reside, em primeira ordem, na relevância estratégica do tema para o sistema financeiro nacional. Os dados pessoais trafegados no ecossistema de open finance não são apenas registros cadastrais ordinários: incluem informações sobre renda, histórico de crédito, hábitos de consumo, perfil de

investimento e padrões comportamentais dos usuários, configurando, em muitos casos, dados sensíveis cuja exposição inadequada pode gerar danos patrimoniais e existenciais graves aos titulares. Bioni (2021), em obra de referência sobre os fundamentos e limites do consentimento na LGPD, sublinha que a complexidade dos fluxos de dados na economia digital supera a capacidade de controle efetivo dos titulares, tornando a arquitetura regulatória e as práticas institucionais de segurança os verdadeiros guardiões da privacidade dos cidadãos. Esse diagnóstico é especialmente pertinente no contexto bancário, onde a assimetria de poder entre as instituições e os usuários é estrutural.

Em segunda ordem, a justificativa ancora-se no fato de que a gestão de riscos de dados sensíveis no open finance ainda carece de tratamento acadêmico sistemático no Brasil, a despeito da urgência do tema. A literatura nacional, embora crescente, tende a analisar isoladamente a regulação de proteção de dados ou a segurança cibernética, sem examinar de forma integrada a interface entre essas duas dimensões no ambiente específico do open finance. Fernandes e Zani (2022), ao investigarem os impactos da LGPD no processo de Know Your Customer (KYC) no contexto do open banking, identificam que o compartilhamento de cadastros entre instituições expõe fragilidades regulatórias ainda não resolvidas, cujo equacionamento exige articulação entre as normas de proteção de dados e as normas de prevenção à lavagem de dinheiro. Essa constatação reforça a necessidade de estudos que adotem uma perspectiva integrada sobre o tema.

Diante do exposto, o presente artigo é orientado pelas seguintes perguntas norteadoras: De que forma o marco regulatório brasileiro disciplina a gestão de riscos de dados sensíveis no ambiente do open finance? Quais são as principais lacunas tecnológicas e organizacionais que comprometem a proteção desses dados nas instituições financeiras? Em que medida a coordenação entre a ANPD e o Banco Central do Brasil é suficiente para garantir a efetividade das normas vigentes?

O objetivo geral deste artigo é analisar os desafios regulatórios e tecnológicos da gestão de riscos de dados sensíveis em instituições financeiras brasileiras no contexto do open finance, identificando as principais lacunas normativas e operacionais e propondo parâmetros analíticos para sua avaliação. Os objetivos específicos são: (i) caracterizar o marco regulatório de proteção de dados sensíveis

aplicável às instituições financeiras no ambiente do open finance; (ii) identificar os principais vetores de risco cibernético associados ao compartilhamento de dados no ecossistema financeiro aberto; e (iii) analisar os desafios de coordenação interinstitucional entre a ANPD e o Banco Central do Brasil na fiscalização do tratamento de dados sensíveis no setor financeiro.

O artigo organiza-se em cinco seções. Após esta introdução, a segunda seção apresenta o referencial teórico em três subtópicos: a regulação de dados sensíveis no sistema financeiro; os vetores de risco no ecossistema do open finance; e os modelos de governança e gestão de riscos de dados. A terceira seção descreve os procedimentos metodológicos adotados. A quarta seção apresenta e discute os principais resultados da pesquisa bibliográfica. A quinta seção expõe as considerações finais, com destaque para as contribuições do estudo, suas limitações e as recomendações para a prática institucional e para políticas públicas.

2 REFERENCIAL TEÓRICO

2.1 Regulação de dados sensíveis no sistema financeiro brasileiro

O conceito de dado sensível no ordenamento jurídico brasileiro ganhou contornos normativos precisos com a promulgação da LGPD, que, em seu artigo 5º, inciso II, define como dados sensíveis aqueles relativos a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018). No contexto financeiro, essa categoria se expande de modo significativo quando se considera que dados bancários como histórico de crédito, padrões de consumo, movimentações financeiras e perfis de investimento, embora não listados expressamente como sensíveis pela lei, permitem a inferência de informações altamente sensíveis sobre a vida dos titulares, tornando sua proteção uma necessidade jurídica e ética de primeira ordem.

A LGPD impõe ao tratamento de dados sensíveis um regime jurídico mais restritivo do que o aplicado aos dados pessoais ordinários. Os artigos 11 e 12 da lei estabelecem um rol taxativo de hipóteses autorizativas para o tratamento dessas informações, exigindo, em regra, o consentimento específico e destacado do titular, ou a demonstração de uma das exceções legais previstas (Brasil, 2018). Para as

instituições financeiras, isso implica a necessidade de revisão contínua de seus processos de tratamento de dados, especialmente nos ambientes de open finance, nos quais o compartilhamento automatizado de informações entre múltiplas instituições dificulta o controle granular sobre quais dados estão sendo efetivamente tratados em cada etapa da cadeia de integração. Bioni (2021) argumenta que o consentimento, como mecanismo de controle do titular sobre seus dados, apresenta limitações estruturais em contextos de assimetria informacional acentuada, como ocorre nas relações entre usuários e instituições financeiras.

O fortalecimento da proteção de dados como valor constitucional veio com a Emenda Constitucional n. 115, de 10 de fevereiro de 2022, que acrescentou ao artigo 5º da Constituição Federal o inciso LXXIX, elevando a proteção de dados pessoais à categoria de direito fundamental autônomo (Brasil, 2022). Esse movimento constitucional não é apenas simbólico: ele impõe ao legislador, ao regulador e às próprias instituições privadas um dever reforçado de conformidade, que se traduz em obrigações de responsabilização e em maior rigor interpretativo quando se trata de restrições ao direito à privacidade dos cidadãos. No plano do sistema financeiro, essa constitucionalização eleva o padrão de responsabilidade das instituições por violações de dados pessoais de clientes, abrindo espaço para a tutela coletiva e constitucional desses direitos em caso de incidentes.

Doneda (2021), ao traçar o panorama histórico da proteção de dados pessoais no Brasil, contextualiza o surgimento da LGPD como o ponto de chegada de um longo processo de amadurecimento regulatório iniciado nas discussões do Ministério da Justiça em 2010 e acelerado pelo advento do Marco Civil da Internet em 2014. Para o autor, a LGPD não é apenas uma lei de conformidade, mas a expressão de uma mudança cultural que coloca o indivíduo como titular soberano de suas informações pessoais, em contraposição ao modelo anterior, no qual os dados eram tratados como recurso das organizações que os coletavam. Essa perspectiva é fundamental para a análise do open finance: ao permitir que os usuários compartilhem seus dados financeiros com qualquer instituição participante de sua escolha, o sistema operacionaliza, no plano técnico, a autodeterminação informacional prevista na legislação, mas também cria novos riscos para o exercício efetivo desse direito.

No âmbito do Banco Central do Brasil, a Resolução CMN n. 4.893, de 26 de fevereiro de 2021, representa o principal instrumento regulatório de segurança cibernética aplicável às instituições financeiras. A norma impõe a estruturação de uma política formal de segurança cibernética, calibrada ao porte e ao perfil de risco de cada instituição, e exige a elaboração de planos de ação e resposta a incidentes, bem como a realização de testes periódicos de continuidade de negócios que contemplem cenários de indisponibilidade causada por ataques cibernéticos (Brasil, 2021a). A norma ancora, em linguagem regulatória, a percepção de que a segurança cibernética deixou de ser uma questão técnica de tecnologia da informação e passou a ser uma responsabilidade de governança corporativa, cuja supervisão compete diretamente ao conselho de administração e à diretoria das instituições.

A sobreposição de competências regulatórias entre a ANPD e o Banco Central do Brasil representa, nesse cenário, um dos desafios mais agudos para as instituições financeiras. Estudos publicados na Revista da PGBC identificaram que o espaço regulatório compartilhado entre a ANPD, o BCB e a Comissão de Valores Mobiliários (CVM) carece de um instrumento de governança formal que coordene as atuações dessas entidades no tocante ao tratamento de dados pessoais no setor financeiro. A ausência desse mecanismo de coordenação cria incerteza regulatória para as instituições e fragmenta a supervisão, reduzindo a efetividade da fiscalização em ambas as esferas. Sobre a relação entre esses reguladores no contexto do open finance, Motta e Rosa (2022) sintetizam bem o problema:

> O Open Banking se apresenta como catalisador de relevantes transformações no sistema financeiro, entre elas a disseminação do uso de inteligência artificial, o que levanta questionamentos se a atual regulação e a Lei Geral de Proteção de Dados oferecem guarida para os titulares de dados em relação aos possíveis riscos do tratamento algorítmico. (Motta; Rosa, 2022, p. 133)

Essa passagem captura, com precisão, a tensão central que percorre o referencial regulatório do open finance: enquanto o sistema avança na sofisticação técnica do compartilhamento de dados e do tratamento algorítmico, o arcabouço normativo ainda não produziu respostas suficientemente granulares para os riscos específicos que essas operações geram para os titulares. Preencher essa lacuna é, portanto, uma das tarefas mais urgentes da agenda regulatória e acadêmica do setor.

2.2 Vetores de risco cibernético no ecossistema do open finance

A arquitetura técnica do open finance, baseada na integração de sistemas por meio de APIs abertas e padronizadas, cria uma topologia de risco diferente daquela observada nos sistemas bancários fechados da era pré-digital. Cada API representa uma interface de comunicação entre instituições distintas, e a cadeia de integrações que sustenta o ecossistema forma uma rede de dependências mútuas na qual as vulnerabilidades de um participante podem comprometer a segurança dos dados de outros. A Associação Open Finance Brasil registra que a taxa de insucesso nas chamadas de API para consentimento no ecossistema atingiu 14,1% no período recente, um indicador que aponta tanto para fragilidades técnicas quanto para tentativas de manipulação do processo de consentimento por agentes mal-intencionados (OpenFinanceBrasil.org.br, 2026). Esse dado revela que a segurança do ecossistema não pode ser avaliada apenas pelo desempenho das instituições individualmente, mas precisa considerar a resiliência sistêmica da cadeia de integração como um todo.

O risco de engenharia social é, nesse contexto, um vetor em especial preocupação. No open finance, o processo de consentimento, que constitui o núcleo jurídico do sistema, pode ser manipulado por meio de técnicas que exploram a confiança dos usuários nas interfaces digitais. Ataques de phishing direcionados a usuários do sistema financeiro aberto procuram induzir consentimentos fraudulentos ou capturar credenciais de acesso, comprometendo a integridade do processo de autorização que a LGPD coloca como fundamento do tratamento legítimo de dados. O NIC.br (2020), em pesquisa sobre a gestão de riscos digitais em empresas brasileiras, constatou que a maioria das organizações nacionais ainda apresenta lacunas significativas nas práticas de conscientização e treinamento de usuários, o que é especialmente preocupante em um ecossistema como o open finance, onde a interação digital dos clientes com múltiplas instituições é intensa e cotidiana.

O risco de terceiros assume proporções sistêmicas no open finance em razão do modelo de negócio dos iniciadores de transação de pagamento (ITPs) e demais participantes não bancários do ecossistema. Fernandes e Zani (2022) demonstram que o compartilhamento de cadastros entre instituições financeiras no contexto do open banking impõe um novo desafio ao processo de KYC, pois a integração de dados

provenientes de diferentes fontes cria incertezas sobre a veracidade e a integridade das informações compartilhadas, abrindo brechas para a utilização de identidades sintéticas e para operações de lavagem de dinheiro por meio de fragmentação de transações. A gestão desse risco exige das instituições participantes não apenas controles técnicos robustos, mas também processos de diligência prévia sobre os parceiros tecnológicos e sobre a qualidade dos dados recebidos.

O Fundo Monetário Internacional, em análise amplamente referenciada na literatura especializada, alertou que o risco cibernético passou a ser a nova ameaça sistêmica à estabilidade financeira global, com o número de ciberataques ao setor triplicando na última década (FMI, 2020). No ecossistema do open finance, esse risco é ampliado pela concentração de dados em infraestruturas compartilhadas e pela interconectividade entre instituições de diferentes portes e graus de maturidade tecnológica. A Pesquisa FEBRABAN de Tecnologia Bancária (FEBRABAN/Deloitte, 2024) registra que os investimentos em segurança cibernética continuam sendo uma prioridade declarada pelos bancos brasileiros, mas a heterogeneidade de capacidades entre as grandes instituições e as fintechs de menor porte cria assimetrias que fragilizam o ecossistema como um todo, já que o nível de segurança do sistema é determinado, em última análise, pelo elo mais fraco de sua cadeia.

Os ataques de ransomware, que sequestram sistemas e exigem pagamento para a restituição do acesso, tornaram-se um dos vetores mais danosos para o setor financeiro na última década e assumem, no contexto do open finance, uma dimensão particularmente grave. Uma instituição vitimada por ransomware pode ter sua capacidade de responder a solicitações de APIs temporariamente interrompida, gerando indisponibilidade em cascata para outras instituições que dependem de seus dados. A Resolução CMN n. 4.893/2021 disciplina explicitamente essa dimensão ao exigir que as instituições elaborem planos de continuidade de negócios que contemplem cenários de indisponibilidade causada por incidentes cibernéticos, mas a efetividade desses planos depende da realização de testes regulares e da integração com os procedimentos de resposta a incidentes dos parceiros tecnológicos (Brasil, 2021a). Esse aspecto sistêmico é, reconhecidamente, o mais difícil de operacionalizar na prática.

Paravela e Domingues (2021) sintetizam com precisão a dualidade que caracteriza o open finance do ponto de vista da segurança: ao mesmo tempo em que o sistema oferece ao consumidor maior controle sobre seus dados e maior acesso a serviços personalizados, ele o expõe a um ecossistema de riscos mais amplo e complexo do que aquele presente no sistema bancário fechado. Para as autoras, a proteção do consumidor no open finance depende de uma arquitetura regulatória que vai além das normas de proteção de dados e da regulação prudencial do BCB, exigindo a integração efetiva entre esses regimes e o estabelecimento de padrões mínimos de segurança aplicáveis a todos os participantes do ecossistema, independentemente de seu porte ou segmento. Esse ponto é central para a presente análise, pois indica que a gestão de riscos de dados sensíveis no open finance é, antes de tudo, um problema de governança sistêmica.

A pesquisa do NIC.br (2022) sobre privacidade e proteção de dados pessoais no Brasil revela que, embora haja avanços formais na implementação de estruturas de governança de dados nas organizações, persiste uma disparidade expressiva entre as grandes instituições, que dispõem de recursos e equipes para uma adequação mais completa, e as organizações menores, que enfrentam obstáculos técnicos e financeiros consideráveis. No setor financeiro, essa disparidade traduz-se em diferenças significativas de maturidade de cibersegurança entre os grandes bancos, que possuem Centros de Operações de Segurança (SOCs) estruturados e equipes especializadas, e as fintechs em estágio inicial, que dependem extensamente de provedores terceirizados para a gestão de suas infraestruturas tecnológicas. Administrar essa assimetria é um dos maiores desafios regulatórios do open finance brasileiro.

2.3 Governança e gestão de riscos de dados sensíveis: modelos e parâmetros

A governança de dados é compreendida, na literatura especializada, como o conjunto estruturado de políticas, processos, papéis e responsabilidades que disciplinam o ciclo de vida dos dados em uma organização, desde a coleta e o armazenamento até o compartilhamento, o uso e a eventual eliminação. No contexto das instituições financeiras, a governança de dados assume uma dimensão estratégica que transcende a conformidade regulatória: ela é o fundamento da confiança do cliente e o instrumento que permite à instituição demonstrar, de forma

auditável, que os dados sob sua custódia são tratados com o rigor e o cuidado exigidos pela legislação e pelas melhores práticas internacionais. Bioni (2021) ressalta que a responsabilização e a prestação de contas, princípio inscrito no artigo 6º, inciso X, da LGPD, implicam a obrigação das organizações de demonstrar, a qualquer tempo e para qualquer interessado, que adotaram medidas eficazes para cumprir as normas de proteção de dados.

O modelo de gestão de riscos de dados sensíveis no open finance precisa contemplar, pelo menos, quatro dimensões inter-relacionadas. A primeira é a dimensão técnica, que envolve os controles de segurança aplicados às interfaces de API, aos sistemas de autenticação, ao armazenamento de dados e às infraestruturas de nuvem. A segunda é a dimensão jurídica e regulatória, que compreende o mapeamento das bases legais de cada operação de tratamento de dados e o acompanhamento contínuo das obrigações decorrentes da LGPD e das normativas do BCB. A terceira é a dimensão organizacional, que abrange a cultura de segurança, a capacitação de equipes e a existência de estruturas de governança com poder efetivo de decisão. A quarta é a dimensão de gestão de terceiros, que exige a avaliação e o monitoramento contínuo dos provedores e parceiros tecnológicos que integram a cadeia de tratamento de dados da instituição. A Resolução CMN n. 4.893/2021 endereça diretamente as dimensões técnica e de terceiros, mas é mais lacônica em relação às dimensões organizacional e jurídica (Brasil, 2021a).

No campo da gestão de riscos de terceiros, o open finance introduz uma complexidade adicional que os modelos tradicionais de avaliação de fornecedores não estão preparados para enfrentar. No ambiente do sistema financeiro aberto, os dados de um cliente podem percorrer uma cadeia de cinco, seis ou mais instituições e provedores em uma única jornada de serviço, cada um com seus próprios controles de segurança, suas próprias políticas de privacidade e seus próprios subprocessadores de dados. A identificação do controlador responsável em cada etapa dessa cadeia, exigida pela LGPD para fins de responsabilização e resposta a incidentes, torna-se um exercício de alta complexidade jurídica e técnica, para o qual a literatura ainda não oferece soluções plenamente satisfatórias. Fernandes e Zani (2022) alertam que a fragilidade na cadeia de KYC causada pelo compartilhamento de cadastros é um exemplo concreto dos riscos que a ausência de padrões claros de responsabilidade na cadeia de dados do open finance pode gerar.

Doneda (2021), ao discutir os fundamentos históricos do direito à proteção de dados no Brasil, observa que a trajetória regulatória nacional foi marcada por uma progressiva ampliação do reconhecimento da autonomia informacional do indivíduo, que evoluiu de uma tutela difusa da privacidade para uma disciplina específica e sistematizada do tratamento de dados. Esse movimento histórico tem implicações diretas para a governança de dados nas instituições financeiras: a proteção de dados deixa de ser vista como uma restrição regulatória ao negócio e passa a ser compreendida como um componente intrínseco da proposta de valor da instituição para seus clientes. No contexto do open finance, essa reconfiguração é especialmente relevante, pois o sistema depende fundamentalmente da confiança dos usuários para funcionar: sem confiança, não há consentimento; sem consentimento, não há compartilhamento de dados; sem compartilhamento, não há ecossistema.

A pesquisa do NIC.br (2022) sobre privacidade e proteção de dados revela que, apesar dos avanços formais na implementação da LGPD, muitas organizações brasileiras ainda carecem de uma abordagem integrada de governança de dados que conecte as obrigações legais às práticas operacionais e à cultura organizacional. O estudo mostra que a designação de encarregados de proteção de dados (DPOs) e a elaboração de políticas de privacidade são os instrumentos mais amplamente adotados, enquanto práticas mais sofisticadas, como a realização de avaliações de impacto à proteção de dados (DPIAs) e a implementação de Privacy by Design, ainda têm penetração limitada nas organizações brasileiras. No setor financeiro, onde a complexidade do tratamento de dados é muito superior à média, essa lacuna de maturidade representa um risco regulatório e reputacional de primeira ordem.

A articulação entre o modelo de governança de dados exigido pela LGPD e os requisitos de segurança cibernética da Resolução CMN n. 4.893/2021 constitui, na prática, o núcleo da gestão de riscos de dados sensíveis no open finance. Sobre essa articulação, vale destacar o que o próprio texto normativo do BCB estabelece como obrigação central das instituições financeiras:

> As instituições referidas no art. 1º devem elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, mencionado no art. 6º, com data base de 31 de dezembro. [...] O relatório mencionado no caput deve ser submetido ao comitê de risco, quando existente, e apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição. (Brasil, 2021a, art. 8º)

A exigência de que o relatório de implementação da política de segurança cibernética seja apreciado pelo conselho de administração evidencia que o legislador regulatório optou por uma arquitetura de governança de caráter descendente, na qual a cibersegurança é tratada como responsabilidade da alta administração e não apenas das equipes técnicas. Essa escolha é coerente com a perspectiva da LGPD sobre a responsabilização e a prestação de contas, mas exige que os conselhos de administração das instituições financeiras desenvolvam competências e instrumentos para avaliar adequadamente os riscos cibernéticos e tomar decisões informadas sobre os investimentos necessários à proteção dos dados de seus clientes.

3 METODOLOGIA

A presente pesquisa adota a abordagem qualitativa de natureza bibliográfica e documental, adequada ao objetivo de analisar criticamente o estado do conhecimento sobre a gestão de riscos de dados sensíveis no open finance brasileiro, a partir das fontes disponíveis na literatura científica e no ordenamento jurídico vigente. A opção pela metodologia qualitativa justifica-se pela necessidade de compreender as relações de sentido entre conceitos normativos, práticas institucionais e categorias analíticas da literatura especializada, sem a pretensão de produzir generalizações estatísticas, mas de oferecer interpretações fundamentadas e analiticamente rigorosas sobre os fenômenos investigados. Essa abordagem metodológica é amplamente reconhecida como adequada para pesquisas de natureza jurídica e de gestão que buscam mapear e sistematizar um campo em rápida evolução normativa e tecnológica.

O levantamento bibliográfico foi conduzido nas seguintes bases de dados e repositórios institucionais: Portal de Periódicos da CAPES; Scientific Electronic Library Online (SciELO); Google Scholar; repositório da Revista da Procuradoria-Geral do Banco Central (Revista PGBC), acessível em revistapgbc.bcb.gov.br; Portal de Legislação do Governo Federal, disponível em planalto.gov.br; Portal do Banco Central do Brasil, em bcb.gov.br; repositório do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), em cetic.br; e Portal do FMI, em imf.org. As buscas foram realizadas com os descritores: 'open finance', 'open banking', 'dados sensíveis', 'LGPD', 'segurança cibernética', 'gestão de riscos', 'proteção de dados', 'instituições

financeiras' e 'Resolução 4.893', utilizados de forma isolada e combinada, em português e inglês.

Os critérios de inclusão adotados para a seleção 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; e (iv) publicação em periódico arbitrado, obra acadêmica reconhecida, por órgão público ou por organização internacional de credibilidade consolidada. Os critérios de exclusão compreenderam: materiais sem autoria identificada, publicações de natureza exclusivamente comercial sem embasamento acadêmico e obras cujos dados bibliográficos completos não foram passíveis de verificação nas bases consultadas. O recorte temporal prioritário das publicações cobre o período de 2018 a 2025, com inclusão de obras anteriores de relevância teórica incontornável.

A análise documental contemplou o exame sistemático da legislação federal pertinente, com destaque para a Lei n. 13.709/2018 (LGPD), a Emenda Constitucional n. 115/2022, a Resolução CMN n. 4.893/2021 e a Resolução Conjunta n. 1/2020, que instituiu o open banking no Brasil. A análise normativa seguiu os cânones da interpretação jurídica sistemática e teleológica, buscando identificar a coerência interna dos diplomas analisados e as eventuais lacunas ou antinomias entre eles. Os relatórios técnicos consultados, produzidos pelo NIC.br, pela FEBRABAN/Deloitte e pelo FMI, foram tratados como fontes documentais primárias de natureza empírica, cujos dados agregam evidências quantitativas e qualitativas ao argumento analítico construído a partir da literatura acadêmica.

A síntese dos resultados foi conduzida pelo método de análise de conteúdo qualitativa, que permitiu identificar, nas fontes consultadas, categorias temáticas recorrentes correspondentes aos objetivos específicos da pesquisa. As categorias analíticas foram: (a) regulação de dados sensíveis e suas bases normativas; (b) vetores de risco cibernético no open finance; (c) lacunas de coordenação interinstitucional entre reguladores; e (d) parâmetros de governança e gestão de riscos de dados. A análise por categorias orientou a estrutura da seção de resultados e garantiu correspondência entre os achados da revisão bibliográfica e os objetivos declarados no início do artigo.

A principal limitação metodológica do estudo reside na ausência de dados primários coletados diretamente junto a gestores, equipes de compliance e profissionais de cibersegurança das instituições financeiras, o que restringiu as conclusões ao plano da análise normativa e da literatura disponível. Pesquisas futuras que combinem a presente abordagem bibliográfica com entrevistas semiestruturadas, surveys com profissionais do setor e estudos de caso de instituições específicas poderão aprofundar os diagnósticos aqui desenvolvidos, conferindo-lhes base empírica primária. Essa limitação é reconhecida como estrutural ao design da pesquisa e está devidamente endereçada nas considerações finais, onde são apontadas as perspectivas de desdobramentos para trabalhos subsequentes.

4 RESULTADOS E DISCUSSÃO

O primeiro resultado relevante desta pesquisa é a confirmação de que o Brasil estruturou, nos últimos anos, um dos arcabouços regulatórios de proteção de dados e segurança cibernética mais robustos da América Latina para o setor financeiro. A combinação da LGPD com a Resolução CMN n. 4.893/2021, a constitucionalização da proteção de dados pela EC n. 115/2022 e a regulamentação específica do open banking pela Resolução Conjunta n. 1/2020 formam um conjunto normativo denso e bem articulado em seus fundamentos. A Pesquisa FEBRABAN de Tecnologia Bancária (FEBRABAN/Deloitte, 2024) confirma que os bancos brasileiros reconhecem esse marco regulatório e declaram a cibersegurança como prioridade estratégica. Contudo, a robustez do arcabouço normativo não se traduz automaticamente em efetividade na gestão de riscos de dados sensíveis, e é precisamente nessa distância entre a norma e a prática que residem as lacunas mais críticas identificadas pela pesquisa.

O segundo achado diz respeito à assimetria tecnológica entre os participantes do ecossistema de open finance, que constitui um dos maiores fatores de risco sistêmico identificados na literatura. Grandes bancos, com Centros de Operações de Segurança (SOCs) estruturados, equipes especializadas em cibersegurança e políticas maduras de governança de dados, convivem no mesmo ecossistema com fintechs em estágio inicial, que dependem extensamente de provedores terceirizados e apresentam graus variáveis de conformidade com as exigências da LGPD e da Resolução CMN n. 4.893/2021. O NIC.br (2022) documenta essa disparidade ao

demonstrar que práticas sofisticadas de proteção de dados, como DPIAs e Privacy by Design, ainda têm penetração limitada nas organizações brasileiras, concentrando-se nas entidades de maior porte. No contexto do open finance, essa assimetria é problemática porque o nível de segurança do ecossistema é determinado, em última análise, pelo elo mais fraco, e não pela média dos participantes.

O terceiro resultado central é a identificação das fragilidades na gestão de risco de terceiros como um vetor de vulnerabilidade crítico no open finance. Fernandes e Zani (2022) demonstram que o compartilhamento de cadastros entre instituições no ambiente do open banking já produziu efeitos concretos sobre os processos de KYC, introduzindo incertezas sobre a veracidade e a integridade das informações compartilhadas e criando brechas exploráveis por organizações criminosas. A Resolução CMN n. 4.893/2021 disciplina o risco de terceiros ao exigir que as instituições realizem avaliação e monitoramento contínuo dos provedores de serviços de tecnologia, mas a efetividade dessa exigência depende de capacidade técnica e de processos de diligência prévia que muitas instituições de menor porte ainda não desenvolveram plenamente. A ausência de padrões setoriais mínimos para a avaliação de provedores de tecnologia no open finance é uma lacuna normativa que merece atenção urgente do regulador.

O quarto achado relevante é a insuficiência dos mecanismos de coordenação entre a ANPD e o Banco Central do Brasil para a supervisão integrada do tratamento de dados sensíveis no setor financeiro. Conforme analisado por Motta e Rosa (2022), o espaço regulatório compartilhado entre os dois reguladores carece de instrumentos formais de coordenação e de protocolos claros para o tratamento de incidentes que envolvam simultaneamente dados pessoais e infraestrutura crítica do sistema financeiro. Essa lacuna impõe às instituições custos regulatórios adicionais, gera incerteza sobre as responsabilidades de cada agente na cadeia de tratamento de dados e fragmenta a supervisão de forma que nenhum dos dois reguladores consegue ter uma visão completa dos riscos sistêmicos associados ao open finance.

Em relação às estratégias de mitigação, a literatura consultada converge na identificação de um conjunto de boas práticas que as instituições mais maduras do setor já adotam e que poderiam ser expandidas para todo o ecossistema do open finance por meio de regulamentação específica. Essas práticas incluem: a realização

de avaliações de impacto à proteção de dados (DPIAs) antes de qualquer nova integração de dados sensíveis; a implementação de Privacy by Design nas interfaces de API, garantindo que a minimização de dados e o controle do titular sejam incorporados na arquitetura técnica do sistema; a criação de protocolos padronizados de notificação de incidentes que integrem as obrigações da LGPD e as exigências do BCB; e o estabelecimento de critérios setoriais mínimos para a avaliação de provedores de tecnologia que participam do ecossistema como subprocessadores de dados (Bioni, 2021; brasil, 2021a).

Por fim, o resultado mais transversal desta pesquisa é a constatação de que a gestão efetiva de riscos de dados sensíveis no open finance não é, fundamentalmente, um problema tecnológico, mas um problema de governança. As tecnologias de segurança necessárias existem e continuam a se aperfeiçoar; o que falta, em muitos casos, é a arquitetura organizacional e institucional que coloque essas tecnologias a serviço de uma política coerente de proteção de dados. Doneda (2021) e Bioni (2021) convergem nessa perspectiva ao argumentar que a efetividade da LGPD depende, em última instância, de uma mudança cultural nas organizações, que incorpore a proteção de dados não como uma restrição regulatória, mas como um valor intrínseco ao relacionamento com os clientes. Para as instituições financeiras que operam no open finance, essa mudança cultural é ao mesmo tempo um imperativo ético, um requisito regulatório e um diferencial competitivo.

5 CONSIDERAÇÕES FINAIS

O presente estudo investigou os desafios regulatórios e tecnológicos da gestão de riscos de dados sensíveis em instituições financeiras brasileiras no contexto do open finance, respondendo ao objetivo geral proposto por meio de uma análise crítica e integrada do arcabouço normativo vigente, dos vetores de risco identificados na literatura especializada e dos modelos de governança disponíveis. A investigação demonstrou que o Brasil construiu um referencial normativo sólido, composto pela LGPD, pela EC n. 115/2022, pela Resolução CMN n. 4.893/2021 e pelas normativas específicas do open finance, mas que a efetividade desse arcabouço depende de avanços ainda pendentes nos planos da coordenação interinstitucional, da maturidade tecnológica dos participantes e da cultura organizacional das instituições.

O primeiro objetivo específico, consistente em caracterizar o marco regulatório de proteção de dados sensíveis no open finance, foi plenamente alcançado. A análise evidenciou que o regime jurídico aplicável ao tratamento de dados sensíveis no setor financeiro é multidimensional, articulando normas constitucionais, legislação geral de proteção de dados e regulação prudencial setorial. A constitucionalização da proteção de dados pela EC n. 115/2022 elevou o padrão de responsabilidade das instituições e criou fundamentos para a tutela coletiva dos direitos dos titulares em caso de violações, o que representa um avanço significativo no plano da efetividade do direito.

O segundo objetivo específico, relativo à identificação dos principais vetores de risco cibernético no open finance, foi igualmente satisfeito. Os vetores mais críticos identificados são: a manipulação do processo de consentimento por engenharia social; o risco sistêmico de terceiros na cadeia de integração de APIs; os ataques de ransomware com efeitos em cascata sobre o ecossistema interconectado; e a concentração de dados em infraestruturas compartilhadas de nuvem com baixa diversificação de provedores. A gestão desses riscos exige das instituições não apenas controles técnicos robustos, mas uma abordagem sistêmica que considere a vulnerabilidade do ecossistema como um todo, e não apenas de cada participante individualmente.

O terceiro objetivo específico, voltado à análise dos desafios de coordenação interinstitucional entre a ANPD e o Banco Central do Brasil, revelou que a ausência de protocolos formais de cooperação entre os dois reguladores é a lacuna institucional mais grave do arcabouço regulatório do open finance brasileiro. A sobreposição de jurisdições sem mecanismos de coordenação adequados fragmenta a supervisão, impõe custos desnecessários às instituições e deixa sem resposta regulatória adequada os incidentes que afetam simultaneamente dados pessoais e a integridade do sistema financeiro.

Do ponto de vista das implicações práticas, a pesquisa aponta para a necessidade urgente de que as instituições financeiras avancem na integração entre suas estruturas de compliance de proteção de dados e suas equipes de cibersegurança, que em muitos casos ainda operam de forma compartimentada. Essa integração é o pré-requisito para a construção de uma governança de dados efetiva, capaz de identificar e mitigar os riscos ao longo de toda a cadeia de tratamento de

dados no open finance, incluindo os processos conduzidos por parceiros e subprocessadores.

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, de harmonização dos requisitos de notificação e de definição das responsabilidades de cada regulador na fiscalização do tratamento de dados sensíveis no setor financeiro. Sem esse protocolo, a fragmentação regulatória tende a se aprofundar à medida que o ecossistema do open finance cresce em escala e complexidade.

Recomenda-se, adicionalmente, que o Banco Central do Brasil e a ANPD desenvolvam conjuntamente um guia de boas práticas de gestão de riscos de dados sensíveis para participantes do open finance, com ênfase nos processos de diligência prévia de provedores de tecnologia e nos critérios para a realização de DPIAs em novas integrações de dados. Esse instrumento de natureza orientativa poderia ser desenvolvido em processo de consulta pública com os participantes do ecossistema, garantindo que os padrões estabelecidos sejam tecnicamente factíveis e economicamente proporcionais ao porte de cada categoria de instituição.

A pesquisa evidenciou, também, a necessidade de investimento em capacitação de profissionais especializados em proteção de dados e cibersegurança no setor financeiro. O déficit de talentos nessa área é reconhecido tanto pelas pesquisas setoriais quanto pela literatura acadêmica, e sua persistência compromete a capacidade das instituições de implementar de forma plena os controles exigidos pela regulação. Iniciativas públicas e privadas de formação e certificação em proteção de dados e segurança cibernética para o setor financeiro são um investimento cujo retorno se mede na redução do risco sistêmico do open finance.

Um aspecto que merece atenção especial em futuras pesquisas é a dimensão algorítmica do risco de dados sensíveis no open finance. O uso crescente de inteligência artificial para a tomada de decisões financeiras a partir de dados compartilhados pelo ecossistema levanta questões sobre discriminação algorítmica, opacidade dos modelos de decisão e capacidade dos titulares de contestar decisões automatizadas que os afetem. Essas questões, ainda insuficientemente tratadas na literatura nacional, deverão assumir crescente importância à medida que o open

finance amadurece e as aplicações de inteligência artificial no setor financeiro se tornam mais sofisticadas.

Entre as limitações do presente estudo, a mais relevante é a ausência de dados primários coletados junto a profissionais das instituições financeiras, o que restringiu as conclusões ao plano do discurso normativo e acadêmico. Estudos futuros que combinem a revisão bibliográfica com pesquisas de campo, estudos de caso e análises comparadas com outros ecossistemas de open finance, como os do Reino Unido e da Austrália, poderão enriquecer significativamente o diagnóstico produzido por esta pesquisa.

Em síntese, a gestão efetiva de riscos de dados sensíveis no open finance brasileiro exige a convergência de um marco regulatório bem coordenado, de uma governança corporativa madura, de capacidade técnica adequada e de uma cultura organizacional genuinamente comprometida com a proteção dos dados de seus clientes. O Brasil avançou substancialmente no plano normativo; o desafio da próxima fase é garantir que esse avanço se traduza em práticas institucionais efetivas, capazes de assegurar que o open finance seja, de fato, um instrumento de empoderamento dos cidadãos e não um vetor de amplificação dos riscos que recaem sobre seus dados mais sensíveis.

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. Disponível em: https://brunobioni.com.br/livros/protecao-de-dados-pessoais/. Acesso em: mar. 2025.

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, armazenamento de dados e 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; CONSELHO MONETÁRIO NACIONAL. Resolução Conjunta n. 1, de 4 de maio de 2020. Dispõe sobre a implementação do Sistema Financeiro Aberto (Open Banking). Brasília: BCB, 2020. Disponível em: https://www.bcb.gov.br. Acesso em: mar. 2025.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (Coords.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 1-30.

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.

FERNANDES, André; ZANI, Juliana. Open Banking e Know Your Customer: impactos da LGPD na veracidade de cadastros compartilhados pelas instituições financeiras. Revista da Procuradoria-Geral do Banco Central, Brasília, v. 16, n. 2, p. 43-58, dez. 2022. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1161. 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.

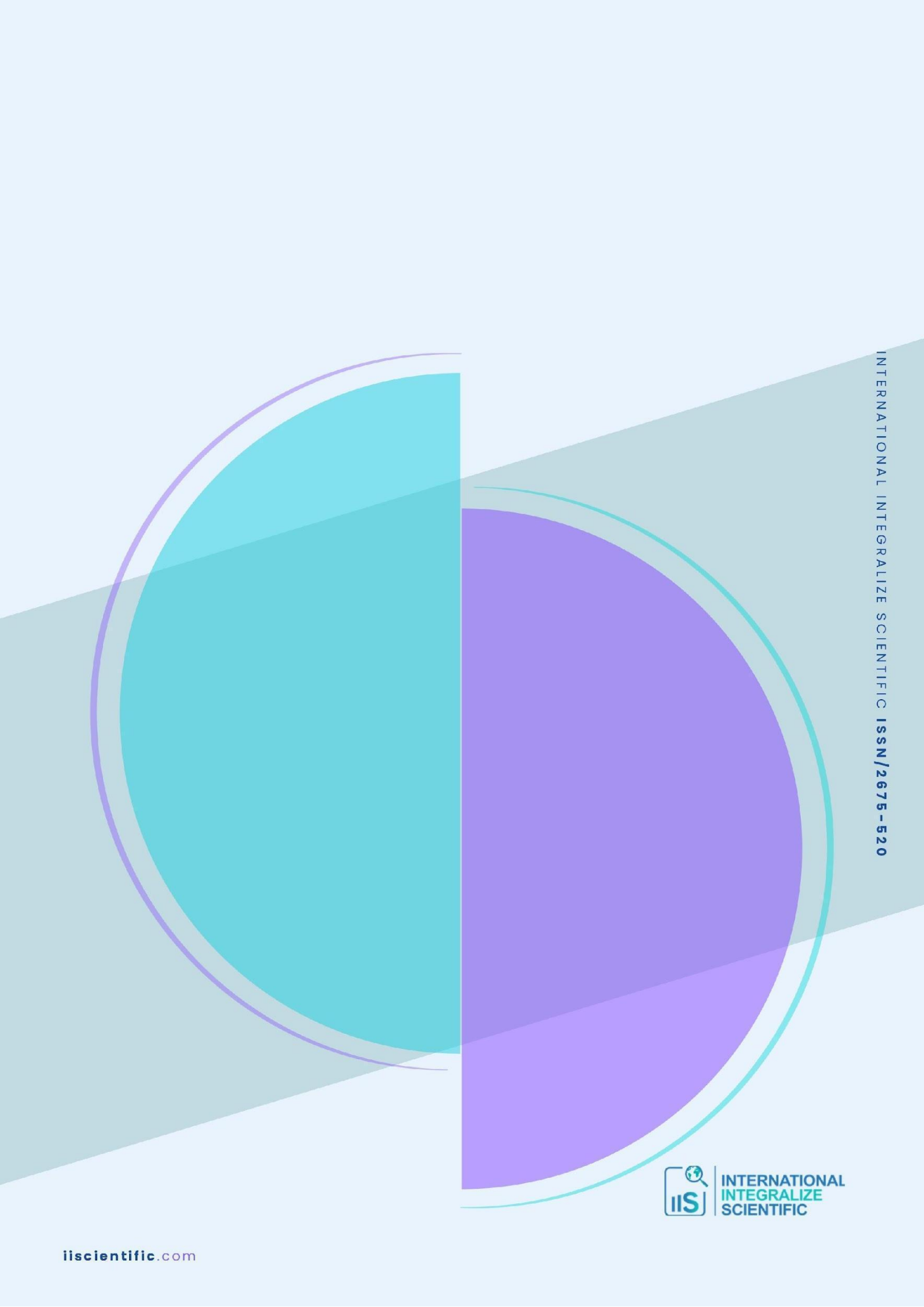
NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Segurança digital: uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf. Acesso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

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: mar. 2025.

OPENFINANCEBRASIL.ORG.BR. Open Finance Brasil: dados e indicadores do ecossistema. Associação Open Finance Brasil, 2026. Disponível em: https://openfinancebrasil.org.br. Acesso em: mar. 2026.

PARAVELA, Tatyana Chiari; DOMINGUES, Juliana Oliveira. Open Banking: a implementação do sistema financeiro aberto no Brasil na perspectiva do consumidor. Revista da Procuradoria-Geral do Banco Central, Brasília, v. 15, n. 2, p. 81-92, dez. 2021. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1133. Acesso em: mar. 2025.

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520



INTERNATIONAL INTEGRALIZE SCIENTIFIC