INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Abril 2026

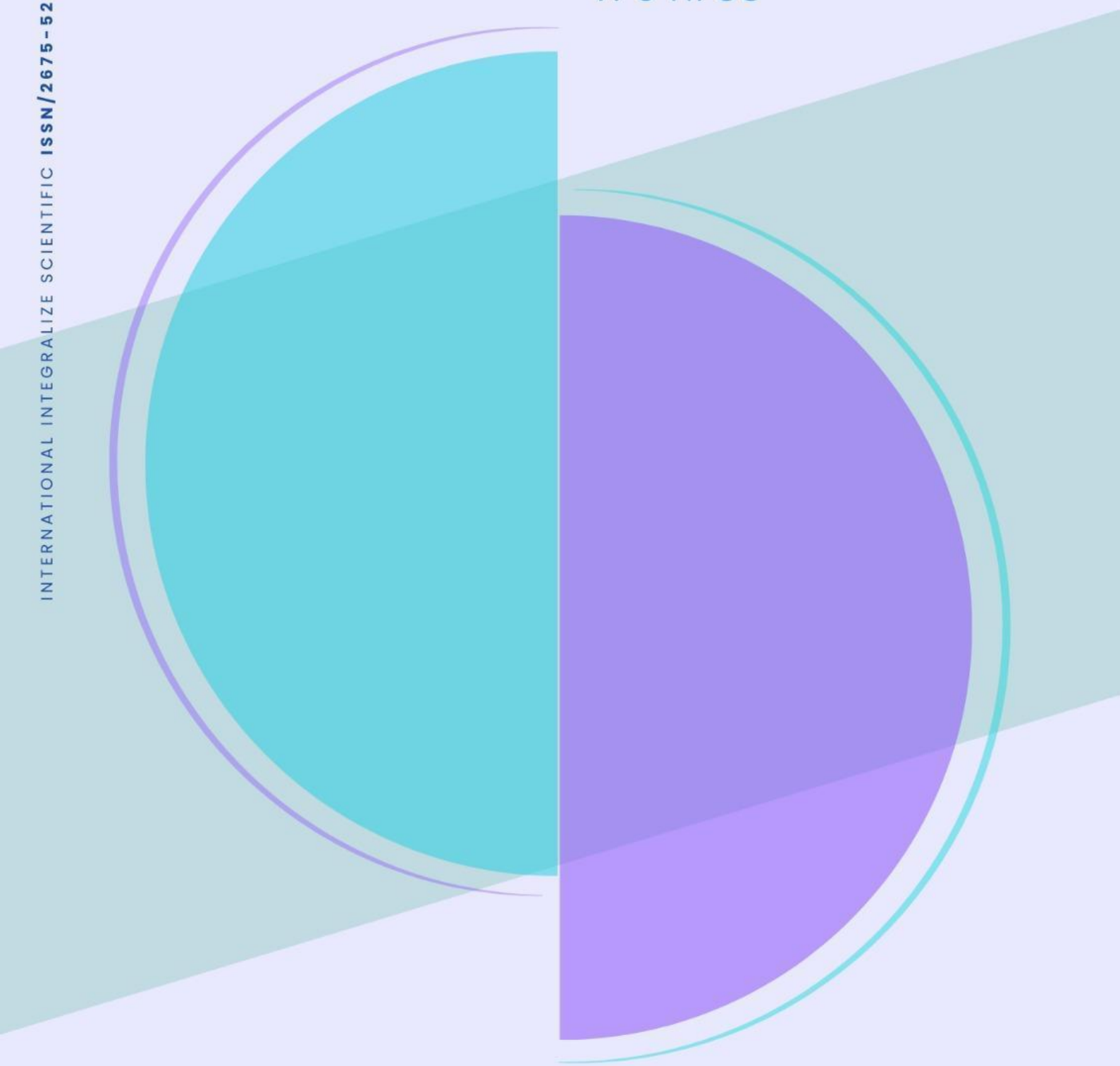
v. 6 n. 58

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

MITIGAÇÃO DE RISCOS CIBERNÉTICOS NO SISTEMA BANCÁRIO BRASILEIRO: GOVERNANÇA DE DADOS, LGPD E RESILIÊNCIA OPERACIONAL

MITIGATION OF CYBER RISKS IN THE BRAZILIAN BANKING SYSTEM: DATA GOVERNANCE, LGPD AND OPERATIONAL RESILIENCE

MITIGACIÓN DE RIESGOS CIBERNÉTICOS EN EL SISTEMA BANCARIO BRASILEÑO: GOBERNANZA DE DATOS, LGPD Y RESILIENCIA OPERACIONAL

RESUMO

O presente artigo analisa a mitigação de riscos cibernéticos no sistema bancário brasileiro, com enfoque na articulação entre a governança de dados, as exigências normativas da Lei Geral de Proteção de Dados Pessoais (LGPD — Lei n. 13.709/2018) e os requisitos de resiliência operacional impostos pelo Banco Central do Brasil, em especial pela Resolução CMN n. 4.893/2021. O estudo investiga de que modo a convergência regulatória entre proteção de dados e segurança cibernética estrutura obrigações jurídicas e técnicas para as instituições financeiras, identificando as principais lacunas de conformidade e os instrumentos disponíveis para o seu enfrentamento. Adota-se como procedimento metodológico a pesquisa bibliográfica e documental de natureza qualitativa, com análise crítica de legislação, normativas setoriais, literatura especializada e relatórios de órgãos nacionais e internacionais. Os resultados evidenciam que o arcabouço regulatório brasileiro, embora inovador, ainda apresenta fragilidades na efetividade das sanções, na coordenação interinstitucional entre a Autoridade Nacional de Proteção de Dados (ANPD) e o Banco Central do Brasil (BCB), e na capacitação técnica de equipes responsáveis pela segurança cibernética nas instituições financeiras. Constata-se, ademais, que a resiliência operacional exige não apenas investimentos tecnológicos, mas a construção de uma cultura organizacional de conformidade, com governança de dados integrada à gestão de riscos. O estudo contribui para o debate acadêmico e institucional sobre a adequação do ordenamento jurídico brasileiro às demandas da economia digital e para o aprimoramento das políticas públicas de cibersegurança no setor bancário.

Palavras-chave: Riscos cibernéticos; LGPD; governança de dados; sistema bancário; resiliência operacional.

ABSTRACT

This article analyzes the mitigation of cyber risks in the Brazilian banking system, focusing on the relationship between data governance, the normative requirements of the General Data Protection Law (LGPD — Law No. 13,709/2018), and the operational resilience requirements imposed by the Central Bank of Brazil, particularly through Resolution CMN No. 4,893/2021. The study investigates how the regulatory convergence between data protection and cybersecurity structures legal and technical obligations for financial institutions, identifying the main compliance gaps and the instruments available to address them. The methodological procedure adopted is qualitative bibliographic and documentary research, with a critical analysis of legislation, sectoral regulations, specialized literature, and reports from national and international bodies. The results show that the Brazilian regulatory framework, while innovative, still presents weaknesses in sanction effectiveness, institutional coordination between the National Data Protection Authority (ANPD) and the Central Bank of Brazil (BCB), and in the technical training of cybersecurity teams in financial institutions. Furthermore, it is found that operational resilience requires not only technological investment but also the construction of an organizational compliance culture, with data governance integrated into risk management. The study contributes to the academic and institutional debate on the adequacy of the Brazilian legal framework to the demands of the digital economy and to the improvement of public policies on cybersecurity in the banking sector.

Keywords: Cyber risks; LGPD; data governance; banking system; operational resilience.

RESUMEN

El presente artículo analiza la mitigación de riesgos cibernéticos en el sistema bancario brasileño, con énfasis en la articulación entre la gobernanza de datos, las exigencias normativas de la Ley General de Protección de Datos Personales (LGPD — Ley n. 13.709/2018) y los requisitos de resiliencia operacional impuestos por el Banco Central de Brasil, en especial a través de la Resolución CMN n. 4.893/2021. El estudio investiga de qué manera la convergencia regulatoria entre protección de datos y seguridad cibernética estructura obligaciones jurídicas y técnicas para las instituciones financieras, identificando las principales brechas de cumplimiento y los instrumentos disponibles para su abordaje. Se adopta como procedimiento metodológico la investigación bibliográfica y documental de naturaleza cualitativa, con análisis crítico de la legislación, normativas sectoriales, literatura especializada e informes de organismos nacionales e internacionales. Los resultados evidencian que el marco regulatorio brasileño, aunque innovador, aún presenta debilidades en la efectividad de las sanciones, en la coordinación interinstitucional entre la Autoridad Nacional de Protección de Datos (ANPD) y el Banco Central de Brasil (BCB), y en la capacitación técnica de los equipos de seguridad cibernética en las instituciones financieras. Se constata, además, que la resiliencia operacional exige no solo inversiones tecnológicas, sino la construcción de una cultura organizacional de cumplimiento, con gobernanza de datos integrada a la gestión de riesgos. El estudio contribuye al debate académico e institucional sobre la adecuación del ordenamiento jurídico brasileño a las demandas de la economía digital y al perfeccionamiento de las políticas públicas de ciberseguridad en el sector bancario.

Palabras clave: Riesgos cibernéticos; LGPD; gobernanza de datos; sistema bancario; resiliencia operacional.

1 INTRODUÇÃO

A digitalização acelerada dos serviços financeiros transformou radicalmente o perfil de risco das instituições bancárias em todo o mundo. No Brasil, a expansão de plataformas digitais, o crescimento do sistema de pagamentos instantâneos (Pix) e a consolidação do open banking ampliaram consideravelmente a superfície de exposição às ameaças cibernéticas. Nesse contexto, a proteção das infraestruturas críticas de informação do setor bancário não se configura apenas como uma questão técnica, mas como um imperativo jurídico, econômico e social de primeira ordem. O Fundo Monetário Internacional (FMI) alertou, em análise publicada em dezembro de 2020, que o número de ciberataques triplicou na última década e que o setor financeiro segue sendo o mais visado, representando uma ameaça direta à estabilidade financeira global (FMI, 2020).

No âmbito nacional, o Brasil se destacou negativamente como o país com maior número de tentativas de ataque cibernético na América Latina no primeiro semestre de 2023, com 23 bilhões de registros, segundo o relatório do FortiGuard Labs da Fortinet (Fortieguard LABS, 2023). Esse quadro evidencia que a vulnerabilidade do sistema bancário brasileiro não decorre apenas da sofisticação das ameaças externas, mas também da insuficiência de controles internos, da

fragmentação regulatória e da escassez de profissionais qualificados em cibersegurança. A ausência de uma estratégia nacional de cibersegurança vinculativa, integrada e multisetorial agrava esse cenário, conforme demonstrado por análises do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cyberbrics, 2023).

O ordenamento jurídico brasileiro respondeu a esse desafio por meio de dois instrumentos normativos centrais: a Lei Geral de Proteção de Dados Pessoais (LGPD — Lei n. 13.709, de 14 de agosto de 2018) e a Resolução CMN n. 4.893, de 26 de fevereiro de 2021, editada pelo Banco Central do Brasil (BACEN). Enquanto a LGPD estabelece um marco abrangente de direitos dos titulares de dados pessoais e obrigações dos agentes de tratamento (Brasil, 2018), a Resolução CMN n. 4.893/2021 impõe às instituições financeiras a estruturação de uma política formal de segurança cibernética, a elaboração de planos de resposta a incidentes e requisitos específicos para a contratação de serviços de computação em nuvem (BRASIL, 2021a). A articulação entre esses dois diplomas normativos constitui o núcleo do problema investigado no presente estudo.

A relevância desta pesquisa decorre da natureza estratégica do setor bancário para a economia nacional e da crescente dependência dos cidadãos em relação a serviços financeiros digitais. Uma falha de segurança em uma grande instituição financeira pode comprometer dados pessoais de milhões de clientes, provocar instabilidade sistêmica e gerar danos irreparáveis à confiança no sistema financeiro. Conforme registrado pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br, 2020), em pesquisa dedicada à gestão de riscos digitais em empresas brasileiras, a maior parte das organizações ainda adota práticas rudimentares de proteção cibernética, desprovidas de uma arquitetura de governança capaz de prevenir, detectar e responder a incidentes de forma sistemática.

Soma-se a esse diagnóstico o fato de que o Brasil apresenta uma escassez crônica de profissionais capacitados em cibersegurança, o que compromete a efetividade das políticas regulatórias mesmo quando bem delineadas. Dados do Fórum Econômico Mundial apontam que, na América Latina, cerca de 42% das organizações manifestam dificuldade na resposta a incidentes cibernéticos, com um déficit estimado entre 2,8 e 4,8 milhões de especialistas no setor globalmente. No

contexto bancário brasileiro, essa realidade se traduz na dependência excessiva de fornecedores terceirizados de tecnologia, cujos controles muitas vezes não são suficientemente auditados pelas instituições contratantes, conforme estabelece a própria Resolução CMN n. 4.893/2021 ao definir critérios rígidos para a terceirização de serviços de processamento e armazenamento de dados (Brasil, 2021a).

Diante desse panorama, esta pesquisa parte das seguintes perguntas norteadoras: de que forma o marco regulatório brasileiro articula a proteção de dados pessoais e a segurança cibernética nas instituições bancárias? Quais são as principais lacunas de conformidade identificadas na literatura especializada e nos relatórios setoriais? Em que medida a governança de dados pode ser concebida como um instrumento estratégico de resiliência operacional no setor bancário? E quais são os principais desafios para a efetividade das sanções previstas na LGPD e na regulação prudencial do BCB?

O objetivo geral desta pesquisa é analisar os mecanismos de mitigação de riscos cibernéticos no sistema bancário brasileiro a partir da interface entre a LGPD, a governança de dados e a Resolução CMN n. 4.893/2021, identificando os principais desafios e oportunidades para a construção de uma resiliência operacional efetiva nas instituições financeiras. Para alcançar esse objetivo, estabelecem-se três objetivos específicos: (i) caracterizar o arcabouço regulatório brasileiro de segurança cibernética e proteção de dados aplicável ao setor bancário; (ii) identificar as principais lacunas de conformidade e os vetores de risco cibernético predominantes no sistema financeiro nacional; e (iii) propor parâmetros analíticos para a avaliação da maturidade em governança de dados como instrumento de resiliência operacional nas instituições financeiras.

O presente artigo estrutura-se em cinco seções. Após esta introdução, apresenta-se o referencial teórico, organizado em três subtópicos: o marco regulatório da segurança cibernética no setor bancário; a governança de dados sob a LGPD; e os conceitos de resiliência operacional aplicados ao contexto financeiro. A terceira seção descreve os procedimentos metodológicos adotados. A quarta seção apresenta e discute os principais resultados da revisão bibliográfica. Por fim, a quinta seção expõe as considerações finais, com destaque para as contribuições do estudo e para as limitações que orientam futuras pesquisas.

2 REFERENCIAL TEÓRICO

2.1 Marco regulatório da segurança cibernética no sistema bancário brasileiro

A regulação da segurança cibernética no sistema bancário brasileiro passou por uma evolução normativa significativa na última década. O ponto de inflexão institucional foi a Resolução n. 4.658, editada pelo Conselho Monetário Nacional em 2018, que obrigou pela primeira vez as instituições financeiras autorizadas a funcionar pelo Banco Central do Brasil a elaborar e implementar políticas formais de segurança cibernética. Esse marco normativo foi revisado e ampliado pela Resolução CMN n. 4.893, de 26 de fevereiro de 2021, que revogou as resoluções anteriores e introduziu exigências mais abrangentes relativas à governança cibernética, ao gerenciamento de riscos e à contratação de serviços em computação em nuvem (Brasil, 2021a).

A Resolução CMN n. 4.893/2021 estabelece que cada instituição financeira deve estruturar sua política de segurança cibernética de forma proporcional ao porte, ao perfil de risco e ao modelo de negócio da organização, garantindo a confidencialidade, a integridade e a disponibilidade das informações (Brasil, 2021a). Trata-se de uma abordagem regulatória baseada em princípios, que preserva a flexibilidade necessária à heterogeneidade do sistema financeiro, que abrange desde grandes bancos de varejo até fintechs em fase de expansão sem, contudo, abrir mão de exigências mínimas universais, como a elaboração de um plano de ação e resposta a incidentes e a revisão anual da política pelo conselho de administração.

Um dos aspectos mais relevantes da referida resolução é a disciplina sobre a contratação de serviços de processamento, armazenamento de dados e computação em nuvem. A norma exige que as instituições realizem avaliação prévia de risco dos fornecedores, verifiquem a aderência destes às políticas de segurança da instituição contratante e garantam direitos de auditoria sobre os prestadores de serviços (Brasil, 2021a). Essa exigência adquiriu especial relevância à medida que as instituições financeiras passaram a depender crescentemente de infraestruturas digitais de terceiros para a prestação de seus serviços essenciais, tornando a cadeia de fornecedores um vetor crítico de risco cibernético, conforme analisado pelo Centro Brasileiro de Estudos em Segurança Digital (Cyberbrics, 2023).

O NIC.br, em estudo publicado em 2020, demonstrou que a maioria das organizações brasileiras, incluindo as do setor financeiro, ainda apresenta maturidade insuficiente em gestão de riscos digitais. A pesquisa revelou que políticas de segurança existem formalmente em muitas empresas, mas carecem de implementação efetiva, monitoramento contínuo e integração com os processos de negócio. Essa constatação é particularmente grave no setor bancário, onde a dependência de sistemas digitais é total e qualquer interrupção pode gerar perdas financeiras expressivas e danos reputacionais irreversíveis (NIC.br, 2020).

A norma regulatória impõe às instituições financeiras a obrigação de elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, o qual deve ser submetido ao comitê de risco e apresentado ao conselho de administração ou à diretoria. Essa exigência de prestação de contas interna representa um mecanismo de accountability corporativo que aproxima a governança cibernética da alta administração, em linha com as recomendações internacionais do Comitê de Supervisão Bancária de Basileia. Observe-se, nesse sentido, a redação do artigo 8º da Resolução CMN n. 4.893/2021:

> Art. 8º 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. [...] § 2º O relatório mencionado no caput deve ser: I - submetido ao comitê de risco, quando existente; e II - apresentado ao conselho de administração ou, na sua inexistência, à diretoria da instituição. (Brasil, 2021a, art. 8º)

A exigência de apresentação do relatório ao conselho de administração evidencia a opção regulatória do BACEN por uma governança cibernética de cima para baixo (top-down), que não admite a delegação integral do tema às equipes técnicas de tecnologia da informação. Essa escolha arquitetônica da norma é coerente com a perspectiva de que o risco cibernético precisa ser tratado com a mesma seriedade atribuída aos riscos operacionais, financeiros e de crédito, integrando-se ao ciclo estratégico das instituições financeiras.

2.2 Governança de dados e a lei geral de proteção de dados pessoais no setor financeiro

A aprovação da Lei n. 13.709, de 14 de agosto de 2018, representou um marco histórico para o ordenamento jurídico brasileiro, ao instituir um regime geral e sistematizado de proteção de dados pessoais inspirado nos modelos europeu (GDPR) e latino-americano. A LGPD estabelece, em seu artigo 6º, dez princípios fundamentais para o tratamento de dados pessoais: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização (Brasil, 2018). Para o setor bancário, esses princípios impõem obrigações concretas de natureza técnica e organizacional, que vão desde o mapeamento dos fluxos de dados pessoais até a implementação de controles de acesso, criptografia e mecanismos de resposta a incidentes.

O jurista Danilo Doneda, uma das principais referências acadêmicas na matéria e um dos elaboradores do anteprojeto que originou a LGPD, sustenta que a proteção de dados pessoais não pode ser compreendida apenas como um conjunto de obrigações procedimentais, mas constitui uma manifestação do direito fundamental à privacidade e à autodeterminação informacional (Doneda, 2021). No setor bancário, essa perspectiva adquire dimensão especialmente delicada, pois as instituições financeiras tratam, em escala massiva, dados pessoais sensíveis de seus clientes, incluindo dados financeiros, históricos de crédito, hábitos de consumo e informações biométricas, cuja exposição indevida pode causar danos patrimoniais e existenciais de difícil reparação.

Bruno Ricardo Bioni, em obra seminal sobre o tema, examina o papel do consentimento e das bases legais para o tratamento de dados pessoais, apontando que o sistema da LGPD não se resume ao consentimento como única hipótese de legitimação, mas contempla múltiplas bases legais que devem ser adequadamente identificadas e documentadas pelos controladores de dados (BIONI, 2021). No contexto bancário, isso significa que os bancos devem delimitar com precisão a base legal de cada operação de tratamento de dados de seus clientes — seja o contrato bancário, a obrigação legal, o legítimo interesse ou o consentimento expresso —, o que exige um processo estruturado de mapeamento e inventário de dados, também denominado data mapping.

A LGPD cria, em seus artigos 46 a 49, um conjunto de obrigações de segurança dirigidas aos agentes de tratamento, controladores e operadores de dados, exigindo que estes adotem medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018). No setor bancário, a interface entre essas obrigações e os requisitos da Resolução CMN n. 4.893/2021 é direta: as mesmas medidas de segurança exigidas pelo BACEN para proteção da infraestrutura digital das instituições financeiras devem ser avaliadas à luz dos deveres de segurança da LGPD, criando uma dupla camada de conformidade regulatória.

O artigo 48 da LGPD institui a obrigação de comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares dos dados, a ser realizada à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares em prazo razoável. Essa obrigação de comunicação tem impacto significativo para as instituições financeiras, que já estão sujeitas a deveres similares junto ao BACEN (Brasil, 2018). A sobreposição de obrigações de reporte a reguladores distintos, ANPD e BCB, sem um protocolo de coordenação interinstitucional claro representa uma das principais lacunas do arcabouço regulatório atual, exigindo dos departamentos jurídicos e de compliance das instituições bancárias um esforço adicional de harmonização.

O NIC.br, em pesquisa realizada em 2021 e publicada em 2022 sobre privacidade e proteção de dados pessoais em organizações brasileiras, revelou que, embora haja avanços formais na implementação de estruturas de governança de dados, como a designação de encarregados de proteção de dados (DPOs) e a elaboração de políticas de privacidade, persiste uma desigualdade expressiva entre as grandes instituições, que dispõem de recursos para adequação plena, e as organizações de menor porte, que enfrentam obstáculos técnicos e financeiros significativos (NIC.br, 2022). No setor bancário, essa assimetria reproduz-se na diferença de maturidade entre os grandes bancos de varejo e as fintechs, embora estas últimas, por sua natureza digital, possam em muitos casos demonstrar maior agilidade na implementação de controles técnicos de segurança.

A consolidação da proteção de dados pessoais como direito fundamental explícito no texto constitucional brasileiro, por meio da Emenda Constitucional n. 115, de 10 de fevereiro de 2022, reforçou o substrato normativo da LGPD e elevou o padrão de responsabilidade das instituições privadas, incluindo os bancos, quanto ao tratamento de dados pessoais (Brasil, 2022). Esse status constitucional implica que eventuais lesões ao direito à proteção de dados passam a ter reparação exigível diretamente com base na Constituição Federal, o que amplia o espectro de responsabilidade civil das instituições financeiras em caso de vazamento de dados ou uso indevido de informações de clientes.

A governança de dados, entendida como o conjunto estruturado de políticas, processos, papéis e responsabilidades que disciplinam o ciclo de vida dos dados em uma organização, emerge, nesse contexto, não apenas como uma exigência de conformidade, mas como um instrumento estratégico de gestão de riscos. Conforme destaca a literatura especializada, a implementação efetiva de uma estrutura de governança de dados no setor bancário compreende, no mínimo: o mapeamento e inventário de todos os dados pessoais tratados; a avaliação de impacto à proteção de dados (DPIA) para atividades de alto risco; a gestão de incidentes com protocolos claros de comunicação interna e externa; e a designação de um DPO com atribuições independentes e acesso direto à alta administração (NIC.br, 2022; Brasil, 2018).

A ANPD, por sua vez, tem avançado na construção de sua agenda regulatória para o biênio 2025-2026, com ênfase em temas como inteligência artificial, dados sensíveis e biométricos, e tratamento de dados de alto risco. Para o setor bancário, a perspectiva de regulamentação setorial específica pela ANPD, em articulação com o BACEN, representa uma oportunidade para a consolidação de parâmetros técnicos mais precisos de conformidade, que reduzam a incerteza regulatória e orientem as instituições na priorização de seus investimentos em segurança. Esse avanço regulatório, contudo, deve ser acompanhado de mecanismos efetivos de supervisão e sanção, cuja ausência ou fragilidade compromete a efetividade do marco normativo vigente.

2.3 Resiliência operacional no setor bancário: Conceitos e fundamentos

O conceito de resiliência operacional, no contexto das instituições financeiras, refere-se à capacidade de uma organização de absorver, adaptar-se e recuperar-se de interrupções operacionais, incluindo aquelas decorrentes de incidentes cibernéticos, sem que os serviços essenciais sejam comprometidos de forma duradoura. Essa capacidade não se limita à dimensão tecnológica, embora esta seja central, mas abrange aspectos humanos, processuais e de governança que determinam a velocidade e a efetividade da resposta institucional a crises. A Resolução CMN n. 4.893/2021 operacionaliza esse conceito ao exigir que as instituições financeiras elaborem testes de continuidade de negócios contemplando cenários de indisponibilidade causada por incidentes cibernéticos (Brasil, 2021a).

A literatura internacional sobre resiliência operacional no setor financeiro aponta três dimensões inter-relacionadas: a capacidade de prevenção, que compreende o conjunto de controles técnicos e procedimentais voltados a reduzir a probabilidade de ocorrência de incidentes; a capacidade de detecção, que envolve sistemas de monitoramento e inteligência de ameaças capazes de identificar incidentes em tempo hábil; e a capacidade de resposta e recuperação, que inclui planos de contingência, backups, protocolos de comunicação de crise e procedimentos de restauração de sistemas (Cyberbrics, 2023). A ausência de maturidade em qualquer dessas dimensões compromete a resiliência total da instituição, independentemente dos investimentos realizados nas demais.

O FMI, em análise divulgada em dezembro de 2020, destacou que a resiliência cibernética do setor financeiro exige não apenas medidas individuais de cada instituição, mas uma abordagem sistêmica que inclua a cooperação entre reguladores, o compartilhamento de informações sobre ameaças e a convergência regulatória internacional (FMI, 2020). Essa perspectiva sistêmica é especialmente relevante para o Brasil, cujo sistema financeiro é altamente concentrado e interconectado, de modo que um incidente cibernético em uma das grandes instituições pode produzir efeitos em cascata sobre todo o ecossistema financeiro, por meio dos mecanismos de contágio operacional.

A Resolução CMN n. 4.893/2021 introduz um elemento particularmente relevante para a análise da resiliência operacional: a disciplina sobre provedores de

serviços de tecnologia da informação (PSTIs) e fornecedores de computação em nuvem. Ao estabelecer critérios rigorosos para a contratação, avaliação e monitoramento desses prestadores, o regulador reconhece que a cadeia de terceiros integra o perímetro de risco das instituições financeiras e que a resiliência operacional não pode ser avaliada isoladamente, sem considerar a vulnerabilidade dos elos externos que sustentam a operação digital das instituições (Brasil, 2021a). Essa abordagem sistêmica do risco de terceiros representa um dos avanços mais significativos da regulação prudencial brasileira no domínio cibernético.

A Resolução nº 4.893 mantém requisitos a respeito da elaboração e divulgação da Política de Segurança Cibernética e do Plano de Ação e de Resposta a Incidentes por parte das instituições. [...] As instituições autorizadas a funcionar pelo Banco Central do Brasil (BACEN) devem obrigatoriamente assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos contemplem a contratação deste tipo de serviço no País ou no exterior. (Brasil, 2021a)

A exigência de que as instituições financeiras apresentem e documentem práticas de governança e procedimentos que contemplem, antes da contratação de serviços em nuvem, a verificação da capacidade e da aderência do prestador às exigências regulatórias evidencia que a resiliência operacional, na concepção adotada pelo regulador brasileiro, pressupõe uma due diligence cibernética ampliada, que vai além da análise financeira tradicional dos fornecedores. Esse movimento alinha-se às melhores práticas internacionais de gestão de riscos de terceiros, como as recomendadas pelo Comitê de Basileia de Supervisão Bancária.

A resiliência operacional não é, portanto, um estado permanente e estático a ser alcançado, mas um processo dinâmico e contínuo de aprendizagem organizacional, adaptação tecnológica e revisão de processos. Nesse sentido, o investimento em capacitação humana, em cultura de segurança e em mecanismos de compartilhamento de informações entre instituições e reguladores constitui uma dimensão fundamental da resiliência que frequentemente é subestimada em favor de soluções puramente tecnológicas (Cyberbrics, 2023; NIC.br, 2020). O sistema bancário brasileiro, para atingir níveis satisfatórios de resiliência operacional cibernética, necessita avançar simultaneamente em todas essas dimensões, sob pena

de construir defesas sólidas em algumas frentes enquanto permanece vulnerável em outras.

3 METODOLOGIA

A presente pesquisa adota a abordagem qualitativa de natureza bibliográfica e documental, adequada ao objetivo de analisar criticamente o arcabouço regulatório e a literatura científica relativa à mitigação de riscos cibernéticos no sistema bancário brasileiro. A opção pela pesquisa qualitativa fundamenta-se na 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 críticas dos fenômenos estudados. Esse método é amplamente consagrado nas ciências jurídicas e na administração pública, conforme registrado pela tradição metodológica da área.

O levantamento bibliográfico foi realizado em bases de dados acadêmicas de acesso aberto e restrito, incluindo o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), o Scientific Electronic Library Online (SciELO), o Google Scholar e o repositório de documentos técnicos do Banco Central do Brasil e da Autoridade Nacional de Proteção de Dados (ANPD). As buscas foram conduzidas com os seguintes descritores, utilizados de forma isolada e combinada: 'risco cibernético', 'segurança cibernética', 'LGPD', 'proteção de dados', 'sistema financeiro', 'governança de dados', 'resiliência operacional', 'Resolução 4.893' e 'instituições financeiras'. O período de cobertura prioritária das publicações consultadas compreende as edições publicadas entre 2018 e 2026, com inclusão de obras anteriores de relevância histórica e teórica incontornável.

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 comprovável; e (iv) publicação em periódicos arbitrados, editoras jurídicas reconhecidas, ou por órgãos públicos e internacionais de reputação consolidada. Os critérios de exclusão abrangeram: 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.

A análise documental compreendeu o estudo sistemático da legislação federal pertinente, em especial a Lei n. 13.709/2018 (LGPD), a Lei n. 12.965/2014 (Marco Civil da Internet) e a Emenda Constitucional n. 115/2022, bem como das normativas infralegais editadas pelo Banco Central do Brasil, notadamente as Resoluções CMN n. 4.658/2018 e n. 4.893/2021. A análise dos documentos normativos seguiu a metodologia da exegese jurídica, orientada pelos cânones da interpretação sistemática, teleológica e histórica, buscando identificar a coerência e as eventuais antinomias entre os diferentes instrumentos regulatórios que incidem sobre o setor bancário.

A síntese dos resultados foi realizada por meio do método de análise de conteúdo qualitativa, que permitiu identificar categorias temáticas recorrentes nas fontes consultadas e agrupá-las em eixos analíticos correspondentes aos objetivos específicos da pesquisa. As categorias identificadas foram: (a) arcabouço regulatório e sua efetividade; (b) vetores de risco cibernético predominantes no setor bancário; (c) lacunas de conformidade com a LGPD e a Resolução CMN n. 4.893/2021; e (d) instrumentos de governança de dados como mecanismo de resiliência operacional. Essa organização categorial orientou a estrutura da seção de resultados e discussão, garantindo correspondência entre os dados coletados e os objetivos declarados.

Entre as limitações metodológicas da pesquisa, destaca-se a ausência de coleta de dados primários junto a instituições financeiras, o que restringiu as conclusões ao plano da análise da literatura e da normativa disponível, sem contemplar a perspectiva dos gestores e profissionais de compliance que atuam diretamente nos processos de adequação regulatória. Reconhece-se, igualmente, que o campo da cibersegurança e da proteção de dados pessoais está em rápida evolução, de modo que estudos futuros baseados em dados empíricos e análise comparada com outros sistemas financeiros poderão aprofundar e eventualmente revisar algumas das conclusões aqui apresentadas. A pesquisa adotou todos os preceitos de integridade científica, com plena identificação das fontes e vedação ao uso de referências não verificáveis.

4 RESULTADOS E DISCUSSÃO

A análise das fontes consultadas evidencia que o Brasil construiu, nos últimos anos, um arcabouço regulatório de segurança cibernética para o setor bancário que se destaca na América Latina por sua abrangência e detalhamento técnico. A Resolução CMN n. 4.893/2021 representa o coroamento de um processo normativo evolutivo iniciado em 2018 e pode ser considerada alinhada às melhores práticas internacionais de supervisão bancária em matéria cibernética. Ao exigir políticas formais, planos de resposta a incidentes, testes de continuidade de negócios e governança de terceiros, o regulador brasileiro demonstra compreensão da natureza sistêmica e multidimensional do risco cibernético (Brasil, 2021a; Cyberbrics, 2023). Contudo, a existência de um marco normativo robusto não é condição suficiente para a efetividade da proteção; é necessário que as instituições disponham de capacidade técnica e organizacional para implementá-lo na prática.

Os dados do NIC.br (2020) revelam que a maioria das organizações brasileiras ainda apresenta maturidade insuficiente em gestão de riscos digitais, com políticas formais que frequentemente não se traduzem em práticas efetivas de monitoramento, resposta e melhoria contínua. No setor bancário, essa realidade é atenuada pelo fato de que as grandes instituições dispõem de recursos tecnológicos e humanos superiores à média, mas permanece preocupante entre as fintechs de menor porte e as cooperativas de crédito, que, embora sujeitas aos mesmos deveres regulatórios, enfrentam restrições de escala que limitam sua capacidade de conformidade plena. A diferença de maturidade entre instituições de distintos portes configura uma assimetria regulatória que pode gerar riscos de concentração sistêmica, pois os elos mais fracos da cadeia financeira tornam-se vetores preferenciais de ataque para agentes maliciosos.

No que diz respeito à interface entre a LGPD e a regulação prudencial do BACEN, os resultados indicam que a ausência de um protocolo formal de coordenação entre a ANPD e o Banco Central do Brasil constitui a principal lacuna institucional do arcabouço regulatório vigente. Enquanto a LGPD atribui à ANPD competência para fiscalizar o tratamento de dados pessoais, inclusive no setor bancário, o BACEN exerce supervisão sobre a gestão de riscos cibernéticos das instituições financeiras por meio de instrumentos próprios. A sobreposição de

jurisdições, sem definição clara de precedência e sem mecanismos de compartilhamento de informações e de coordenação de sanções, impõe às instituições custos regulatórios adicionais e gera incerteza sobre como atender simultaneamente às exigências de ambos os reguladores, especialmente em situações de incidentes que envolvam simultaneamente dados pessoais e infraestrutura crítica (Brasil, 2018; Brasil, 2021a).

O segundo vetor de risco identificado na literatura é a dependência excessiva de fornecedores terceirizados de tecnologia. O FMI (2020) alertou que a concentração de serviços de processamento e armazenamento de dados em poucos provedores de computação em nuvem cria riscos de concentração sistêmica no setor financeiro global, pois uma falha ou ataque a um desses provedores pode afetar simultaneamente dezenas de instituições. No Brasil, a Resolução CMN n. 4.893/2021 reconhece esse risco ao estabelecer critérios para a avaliação e monitoramento contínuo dos prestadores de serviços relevantes, incluindo a possibilidade de o BACEN vetar ou impor restrições à contratação de provedores que não atendam às exigências normativas (Brasil, 2021a). A efetividade dessa prerrogativa regulatória, contudo, depende da capacidade operacional de supervisão do BACEN, que ainda enfrenta desafios na fiscalização de uma cadeia de terceiros cada vez mais extensa e complexa.

Os resultados da pesquisa indicam, ademais, que a dimensão humana do risco cibernético, frequentemente subestimada em favor de soluções tecnológicas, constitui um dos principais vetores de vulnerabilidade do sistema bancário. A engenharia social, o phishing e a exploração de credenciais de colaboradores representam, historicamente, os pontos de entrada mais comuns nos ambientes corporativos. A Resolução CMN n. 4.893/2021 contempla essa dimensão ao exigir que as instituições incluam em sua política de segurança cibernética mecanismos de conscientização e capacitação de usuários (Brasil, 2021a). A efetividade desses mecanismos, porém, depende de uma cultura organizacional de segurança que transcende a mera realização de treinamentos periódicos e exige o engajamento genuíno da liderança e a integração da segurança em todos os processos de negócio.

Por fim, a análise evidencia que a governança de dados, quando adequadamente estruturada, funciona como um mecanismo transversal de resiliência

operacional, ao proporcionar às instituições financeiras uma visibilidade abrangente sobre seus ativos de informação, seus riscos e suas vulnerabilidades. A implementação de um programa robusto de governança de dados no setor bancário, compreendendo mapeamento de dados, avaliação de impacto à proteção de dados (DPIA), gestão de incidentes e monitoramento contínuo, permite que a instituição responda com maior agilidade e precisão a incidentes cibernéticos, minimize os danos e demonstre aos reguladores o cumprimento de seus deveres de diligência (Bioni, 2021; NIC.br, 2022; Brasil, 2018). Essa constatação reforça a tese central do presente estudo: a mitigação efetiva de riscos cibernéticos no sistema bancário brasileiro requer não apenas o cumprimento formal das normas existentes, mas a internalização de uma cultura de governança de dados que integre proteção, segurança e resiliência como dimensões indissociáveis da gestão institucional.

5 CONSIDERAÇÕES FINAIS

O presente estudo demonstrou que o Brasil dispõe de um arcabouço regulatório progressivo e tecnicamente articulado para a gestão de riscos cibernéticos no sistema bancário, materializado principalmente pela Resolução CMN n. 4.893/2021 e pela LGPD. A articulação entre essas duas esferas normativas, a prudencial e a de proteção de dados, constitui uma exigência de conformidade dupla que as instituições financeiras precisam gerenciar de forma integrada, sob pena de enfrentar responsabilizações simultâneas por parte do BACEN e da ANPD. A pesquisa respondeu ao objetivo geral proposto ao identificar os principais mecanismos de mitigação de riscos cibernéticos disponíveis no ordenamento jurídico e na literatura especializada, e ao mapear as lacunas que ainda comprometem sua efetividade plena.

O primeiro objetivo específico, caracterizar o arcabouço regulatório brasileiro de segurança cibernética e proteção de dados aplicável ao setor bancário, foi plenamente alcançado. A análise revelou que a Resolução CMN n. 4.893/2021 representa uma evolução normativa significativa em relação às resoluções que a precederam, ao introduzir exigências mais detalhadas de governança cibernética, controle de terceiros e transparência perante a alta administração. A LGPD, por sua vez, estabelece um conjunto de princípios e deveres de segurança que se superpõem

às exigências prudenciais do BACEN, criando uma dupla camada de proteção jurídica para os dados dos clientes das instituições financeiras.

O segundo objetivo específico, identificar as principais lacunas de conformidade e os vetores de risco cibernético predominantes no sistema financeiro nacional, foi igualmente alcançado. As lacunas mais significativas identificadas na literatura são: a ausência de coordenação formal entre a ANPD e o BACEN; a assimetria de maturidade entre grandes instituições e fintechs de menor porte; a insuficiência dos mecanismos de supervisão sobre a cadeia de terceiros; e a dimensão humana do risco cibernético, frequentemente negligenciada em estratégias centradas em soluções tecnológicas. Os vetores de risco mais críticos incluem os ataques de ransomware, a engenharia social, as falhas de segurança em provedores terceirizados e a concentração de infraestruturas críticas em poucos prestadores de computação em nuvem.

O terceiro objetivo específico, propor parâmetros analíticos para a avaliação da maturidade em governança de dados como instrumento de resiliência operacional, foi abordado a partir da síntese das principais contribuições da literatura especializada. Os parâmetros identificados são: (i) existência e qualidade do mapeamento de dados pessoais; (ii) implementação de DPIA para operações de alto risco; (iii) efetividade dos protocolos de gestão e comunicação de incidentes; (iv) grau de integração da governança de dados com a gestão de riscos corporativos; e (v) maturidade dos processos de avaliação e monitoramento de fornecedores terceirizados. Esses parâmetros oferecem às instituições financeiras e aos reguladores um referencial prático para avaliar a adequação de suas estruturas de governança de dados ao nível de risco de suas operações.

Do ponto de vista das implicações práticas, a pesquisa sugere que as instituições financeiras precisam avançar na integração entre suas áreas de segurança da informação, compliance, jurídico e tecnologia da informação, de modo a construir uma resposta coordenada às exigências regulatórias que supere a compartimentação departamental. A criação de comitês interfuncionais de governança cibernética, com participação ativa da alta administração e reporte regular ao conselho de administração, configura uma boa prática alinhada tanto à Resolução CMN n. 4.893/2021 quanto às orientações da LGPD.

No plano das políticas públicas, o estudo sugere a conveniência de uma regulamentação conjunta entre a ANPD e o BACEN que estabeleça protocolos claros de coordenação, compartilhamento de informações e harmonização de requisitos de reporte de incidentes para o setor bancário. Essa iniciativa reduzeria os custos de conformidade das instituições e aumentaria a efetividade da supervisão regulatória, ao eliminar sobreposições desnecessárias e garantir que os recursos das autarquias sejam empregados de forma complementar e sinérgica.

A pesquisa também aponta para a necessidade urgente de investimento em formação e capacitação de profissionais de cibersegurança no Brasil, em parceria entre o governo, o setor privado e as instituições de ensino superior. O déficit de especialistas qualificados compromete tanto a efetividade da regulação quanto a capacidade das instituições financeiras de implementar controles técnicos adequados. Programas de formação continuada, certificações profissionais reconhecidas e incentivos fiscais para empresas que investem em educação em segurança cibernética são instrumentos de política pública que merecem atenção prioritária.

Uma das contribuições mais relevantes do presente estudo para o debate acadêmico é a demonstração de que a governança de dados não pode ser compreendida como um fim em si mesmo ou como um mero exercício de conformidade regulatória. Quando adequadamente concebida e implementada, a governança de dados constitui uma infraestrutura de inteligência organizacional que permite à instituição financeira conhecer, proteger e valorizar seus ativos de informação, reduzir sua exposição a riscos cibernéticos e responder com maior agilidade e precisão a crises operacionais.

Entre as limitações do estudo, destaca-se a ausência de dados primários coletados diretamente junto a gestores e equipes de compliance de instituições financeiras brasileiras, o que restringiu a análise ao plano do discurso normativo e acadêmico. Pesquisas futuras que combinem a revisão bibliográfica com entrevistas estruturadas, surveys com profissionais do setor e estudos de caso de instituições específicas poderão enriquecer consideravelmente o diagnóstico sobre a efetividade das práticas de governança cibernética no sistema bancário brasileiro.

Outra limitação relevante é a velocidade de evolução do campo objeto de estudo. As ameaças cibernéticas, as tecnologias de proteção e o próprio marco

regulatório estão em permanente transformação, o que torna necessária a atualização periódica dos diagnósticos e recomendações aqui apresentados. Em particular, a emergência da inteligência artificial como ferramenta tanto de ataque quanto de defesa cibernética promete alterar substancialmente o perfil de risco do setor bancário nos próximos anos, demandando respostas regulatórias e acadêmicas ainda em construção.

Em síntese, a mitigação efetiva de riscos cibernéticos no sistema bancário brasileiro exige a confluência de um marco regulatório robusto, de uma governança de dados integrada e madura, de capacidade técnica e humana adequada e de uma cultura organizacional genuinamente comprometida com a segurança. O arcabouço normativo vigente, LGPD e Resolução CMN n. 4.893/2021, fornece os fundamentos jurídicos necessários; cabe às instituições financeiras, aos reguladores e à academia a tarefa de traduzi-los em práticas efetivas de proteção e resiliência, contribuindo para a construção de um sistema financeiro mais seguro, confiável e sustentável.

6 REFERÊNCIAS

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

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. 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. 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 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, DF: Banco Central do Brasil, 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 contratação de serviços de processamento e armazenamento de dados e de computação em nuvem pelas instituições de pagamento. Brasília, DF: Banco Central do Brasil, 2021b. Disponível em: https://www.bcb.gov.br. Acesso em: mar. 2025.

CYBERBRICS. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório. Artigos para discussão, n. 1. Rio de Janeiro: CyberBRICS, 2023. Disponível em: https://cyberbrics.info/wp-content/uploads/2023/03/Agenda-de-politicas-publicas-em-ciberseguranca-consolidado-primeira-final.pdf. Acesso em: mar. 2025.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

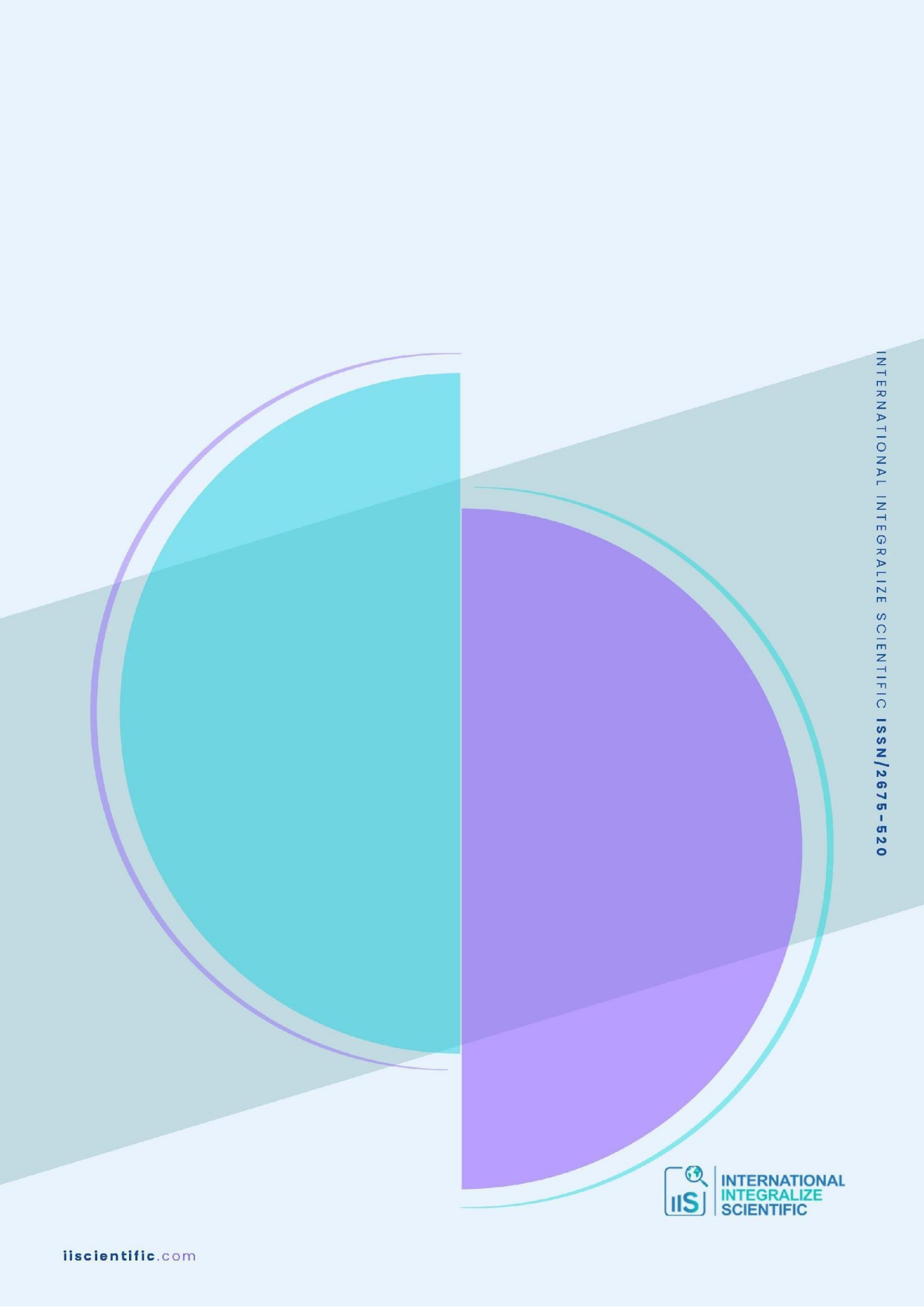
FUNDO MONETÁRIO INTERNACIONAL. O risco cibernético é a nova ameaça à estabilidade financeira. Blog do FMI, 7 dez. 2020. Disponível em: https://www.imf.org/pt/blogs/articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability. Acesso em: mar. 2025.

FORTINET. FortiGuard Labs. Threat Intelligence Brief: Brasil — 1º semestre de 2023. Sunnyvale: Fortinet, 2023. Disponível em: https://www.fortinet.com. Acesso em: mar. 2025.

NIC.BR. Núcleo de Informação e Coordenação do Ponto 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.

NIC.BR. Núcleo de Informação e Coordenação do Ponto 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.

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520



INTERNATIONAL INTEGRALIZE SCIENTIFIC