INTERNATIONAL
INTEGRALIZE
SCIENTIFIC

Abril 2026

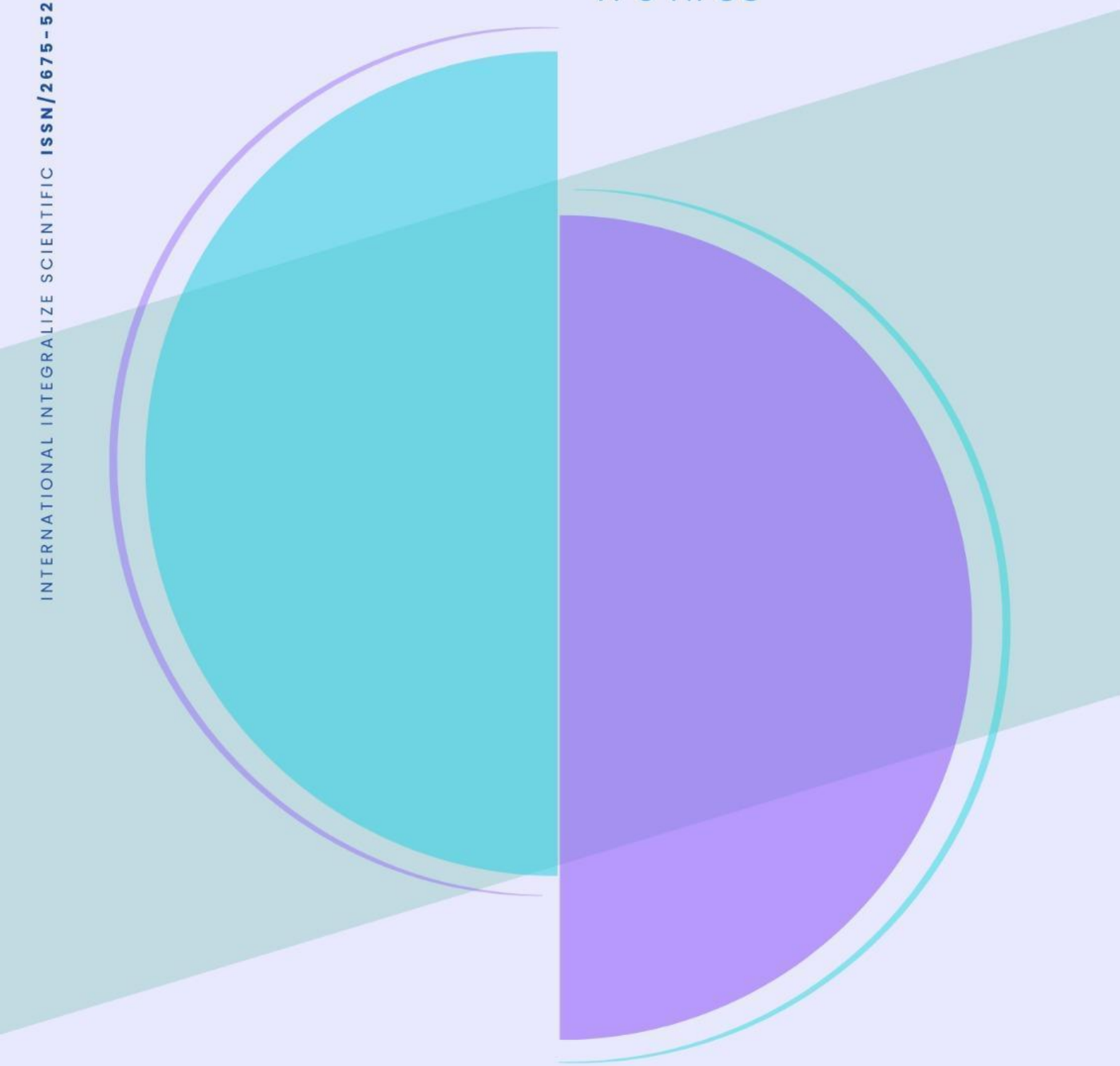
v. 6 n. 58

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

ARQUITETURAS DE SEGURANÇA E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS EM BANCOS BRASILEIROS: CONFORMIDADE, MONITORAMENTO E CONTINUIDADE DE NEGÓCIOS

SECURITY ARCHITECTURES AND CYBERTHREAT MITIGATION IN BRAZILIAN BANKS: COMPLIANCE, MONITORING AND BUSINESS CONTINUITY

ARQUITECTURAS DE SEGURIDAD Y MITIGACIÓN DE AMENAZAS CIBERNÉTICAS EN BANCOS BRASILEÑOS: CUMPLIMIENTO, MONITOREO Y CONTINUIDAD DEL NEGOCIO

RESUMO

O presente artigo analisa as arquiteturas de segurança adotadas por bancos brasileiros para a mitigação de ameaças cibernéticas, examinando como as dimensões de conformidade regulatória, monitoramento contínuo e continuidade de negócios se articulam na construção de ambientes financeiros digitais mais seguros e resilientes. A pesquisa adota abordagem qualitativa de natureza bibliográfica e documental, com análise crítica da legislação vigente, das regulamentações do Banco Central do Brasil, de normas técnicas internacionais como a ABNT NBR ISO/IEC 27001 e da produção acadêmica especializada sobre segurança cibernética no setor financeiro. O estudo reconhece que o setor bancário brasileiro ocupa posição de destaque na adoção de tecnologias digitais, tornando-se simultaneamente um dos ambientes mais expostos a ataques cibernéticos sofisticados, que evoluem em velocidade e complexidade superiores às respostas institucionais tradicionais. A revisão da literatura evidencia que a arquitetura de segurança eficaz nas instituições financeiras brasileiras não se reduz ao conjunto de tecnologias implementadas, mas compreende um sistema integrado de políticas, processos, controles e culturas organizacionais que operam em conformidade com um arcabouço normativo de múltiplas camadas, composto pela Lei Geral de Proteção de Dados, pelas resoluções do Banco Central e pelos padrões internacionais de gestão da segurança da informação. Os resultados apontam que a efetividade das arquiteturas de segurança bancária depende da articulação entre três pilares complementares: a conformidade proativa com as exigências regulatórias, o monitoramento contínuo e inteligente das ameaças e a manutenção de planos robustos de continuidade de negócios, que garantam a resiliência operacional mesmo em cenários de incidentes graves. Conclui-se que o amadurecimento das práticas de segurança cibernética no setor bancário brasileiro exige investimentos sustentados em tecnologia, pessoas e governança, superando a perspectiva meramente reativa para alcançar uma postura preventiva e estratégica de gestão de riscos digitais.

Palavras-chave: Segurança cibernética; bancos brasileiros; arquitetura de segurança; continuidade de negócios; conformidade regulatória.

ABSTRACT

This article analyzes the security architectures adopted by Brazilian banks for cyberthreat mitigation, examining how the dimensions of regulatory compliance, continuous monitoring and business continuity articulate in building safer and more resilient digital financial environments. The research adopts a qualitative approach of bibliographic and documentary nature, with critical analysis of current legislation, Central Bank of Brazil regulations, international technical standards such as ABNT NBR ISO/IEC 27001, and specialized academic production on cybersecurity in the financial sector. The study recognizes that the Brazilian banking sector occupies a prominent position in the adoption of digital technologies, simultaneously becoming one of the environments most exposed to sophisticated cyberattacks, which evolve in speed and complexity superior to traditional institutional responses. The literature review shows that effective security architecture in Brazilian financial institutions is not reduced to the set of technologies implemented, but comprises an integrated system of policies, processes, controls and organizational cultures that operate in compliance with a multi-layered normative framework. The results indicate that the effectiveness of banking security architectures depends on the articulation of three complementary pillars: proactive compliance with regulatory requirements, continuous and intelligent threat monitoring, and the maintenance of robust business continuity plans that ensure operational resilience even in serious incident scenarios. It is concluded that the maturation of cybersecurity

practices in the Brazilian banking sector requires sustained investments in technology, people and governance, moving beyond a merely reactive perspective to achieve a preventive and strategic posture of digital risk management.
Keywords: Cybersecurity; brazilian banks; security architecture; business continuity; regulatory compliance.

RESUMEN

El presente artículo analiza las arquitecturas de seguridad adoptadas por los bancos brasileños para la mitigación de amenazas cibernéticas, examinando cómo las dimensiones de cumplimiento regulatorio, monitoreo continuo y continuidad del negocio se articulan en la construcción de entornos financieros digitales más seguros y resilientes. La investigación adopta un enfoque cualitativo de naturaleza bibliográfica y documental, con análisis crítico de la legislación vigente, las regulaciones del Banco Central de Brasil, normas técnicas internacionales como la ABNT NBR ISO/IEC 27001 y la producción académica especializada en ciberseguridad en el sector financiero. El estudio reconoce que el sector bancario brasileño ocupa una posición destacada en la adopción de tecnologías digitales, convirtiéndose simultáneamente en uno de los entornos más expuestos a ciberataques sofisticados que evolucionan a una velocidad y complejidad superiores a las respuestas institucionales tradicionales. Los resultados indican que la efectividad de las arquitecturas de seguridad bancaria depende de la articulación de tres pilares complementarios: el cumplimiento proactivo de los requisitos regulatorios, el monitoreo continuo e inteligente de las amenazas y el mantenimiento de planes robustos de continuidad del negocio. Se concluye que la maduración de las prácticas de ciberseguridad en el sector bancario brasileño requiere inversiones sostenidas en tecnología, personas y gobernanza.
Palabras clave: Ciberseguridad; bancos brasileños; arquitectura de seguridad; continuidad del negocio; cumplimiento regulatorio.

1 INTRODUÇÃO

O setor bancário brasileiro é reconhecido internacionalmente pela sofisticação tecnológica de sua infraestrutura digital, acumulada ao longo de décadas de investimento contínuo em automação, digitalização e inovação financeira. Esse protagonismo tecnológico, porém, coloca os bancos nacionais em uma posição de dupla exposição: ao mesmo tempo em que usufruem dos ganhos de eficiência, escala e alcance proporcionados pela digitalização, tornam-se alvos preferenciais de agentes maliciosos que buscam explorar as vulnerabilidades inerentes a sistemas complexos e altamente interconectados. Semola (2014) observa que a segurança da informação nas organizações modernas não pode mais ser concebida como um conjunto estático de proteções perimetrais, mas deve ser entendida como um processo dinâmico de gestão de riscos que se adapta continuamente ao ambiente de ameaças em evolução, premissa que é especialmente pertinente para o setor bancário, onde os ativos informacionais têm valor patrimonial e estratégico imediato.

A Lei Geral de Proteção de Dados Pessoais, em vigor desde setembro de 2020, impôs ao setor financeiro um novo patamar de exigências relacionadas ao

tratamento e à proteção dos dados de seus clientes, ampliando o escopo das obrigações de segurança que as instituições bancárias precisam atender. Paralelamente, o Banco Central do Brasil consolidou seu aparato regulatório de segurança cibernética por meio da Resolução n. 4.658, de 26 de abril de 2018, que determinou a implementação de políticas de segurança cibernética e de planos de ação e de resposta a incidentes em todas as instituições autorizadas a funcionar no sistema financeiro nacional. Pinheiro (2021) destaca que a interação entre a LGPD e a regulação prudencial do Banco Central criou um ambiente normativo de elevada complexidade para o setor financeiro, pois as obrigações de segurança impostas pelos dois marcos normativos são complementares mas não idênticas, exigindo que as instituições desenvolvam programas de conformidade que contemplem ambas as perspectivas de forma integrada e coerente.

A Pesquisa FEBRABAN de Tecnologia Bancária de 2022 evidenciou que os bancos brasileiros investiram volumes crescentes em segurança cibernética nos anos anteriores à publicação do relatório, com tendência de aceleração dos investimentos em ferramentas de detecção e resposta a incidentes, inteligência de ameaças e proteção de ambientes em nuvem. Esse cenário de investimento crescente, contudo, não eliminou a exposição dos bancos a ataques bem-sucedidos, o que sugere que a questão da segurança cibernética bancária não se resolve apenas pelo volume de recursos alocados, mas exige uma abordagem arquitetural que organize os investimentos em torno de uma estratégia coerente e orientada por riscos. Bioni (2021) ressalta que a proteção dos dados pessoais dos clientes bancários é um imperativo não apenas regulatório, mas ético e comercial, pois a confiança do consumidor nos serviços financeiros digitais depende diretamente da percepção de que suas informações são tratadas com segurança e respeito, o que torna a segurança cibernética um componente central da proposta de valor dos bancos no ambiente digital. Como os bancos brasileiros têm estruturado suas arquiteturas de segurança para responder a esse ambiente de ameaças em permanente evolução? De que forma os requisitos de conformidade, monitoramento e continuidade de negócios se articulam nessas arquiteturas?

A justificativa deste estudo reside, em primeira instância, na crescente sofisticação e frequência dos ataques cibernéticos direcionados ao setor financeiro brasileiro, fenômeno documentado pelos relatórios anuais do Centro de Estudos,

Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que registram volumes crescentes de incidentes reportados envolvendo instituições financeiras, com destaque para ataques de ransomware, phishing direcionado, fraudes em ambientes de pagamento digital e exploração de vulnerabilidades em APIs de Open Finance. Doneda (2019) argumenta que a proteção dos dados pessoais nas sociedades digitais contemporâneas demanda uma abordagem sistêmica que vai além da conformidade formal com normas, alcançando a construção de arquiteturas organizacionais e tecnológicas que incorporam a privacidade e a segurança como valores constituintes dos sistemas, e não como requisitos externos adicionados a posteriori. Essa perspectiva é diretamente aplicável ao setor bancário, onde a arquitetura de segurança precisa ser pensada desde o projeto dos sistemas e dos processos, e não como uma camada de proteção sobreposta a estruturas desenvolvidas sem consideração pelos riscos de segurança.

A relevância científica do tema justifica-se, em segundo lugar, pela insuficiência da produção acadêmica brasileira que analise de forma integrada as dimensões técnica, normativa e de gestão de riscos das arquiteturas de segurança cibernética em bancos, tema que frequentemente é tratado de forma fragmentada na literatura nacional. Os estudos jurídicos se concentram na análise da LGPD e das regulamentações do Banco Central sem aprofundar as implicações técnicas dessas normas para a arquitetura dos sistemas bancários, enquanto os trabalhos de tecnologia da informação descrevem soluções e frameworks de segurança sem articulá-los com o contexto regulatório e com as especificidades operacionais do setor bancário. Tepedino, Frazão e Oliva (2020) apontam que a efetividade dos marcos normativos de proteção de dados depende de sua tradução em práticas organizacionais e técnicas concretas, o que exige a produção de pesquisas que integrem as perspectivas jurídica, tecnológica e de gestão em uma análise que seja ao mesmo tempo teoricamente rigorosa e praticamente relevante. Que lacunas nos programas de conformidade regulatória dos bancos brasileiros explicam a persistência de vulnerabilidades significativas mesmo em um ambiente de investimento crescente em segurança?

Este artigo tem como objetivo geral analisar as arquiteturas de segurança adotadas por bancos brasileiros para a mitigação de ameaças cibernéticas, examinando como as dimensões de conformidade regulatória, monitoramento

contínuo e continuidade de negócios se articulam na construção de ambientes financeiros digitais seguros e resilientes. Para alcançar esse propósito amplo, definem-se os seguintes objetivos específicos: (a) examinar o arcabouço normativo que regula a segurança cibernética no setor bancário brasileiro, identificando as principais obrigações de segurança, monitoramento e continuidade operacional impostas às instituições; (b) analisar as principais categorias de ameaças cibernéticas que afetam os bancos brasileiros e os modelos arquiteturais de segurança recomendados para sua mitigação; (c) identificar as práticas de monitoramento contínuo e de continuidade de negócios que a literatura e os normativos regulatórios reconhecem como mais eficazes para a resiliência operacional das instituições financeiras.

Para atender a esses objetivos, o artigo está organizado em cinco seções. A presente introdução contextualiza o problema, apresenta a justificativa da pesquisa e delimita os objetivos. A segunda seção desenvolve o referencial teórico em três subtópicos: o primeiro examina os fundamentos normativos e técnicos das arquiteturas de segurança em bancos brasileiros; o segundo analisa as principais categorias de ameaças cibernéticas e os modelos arquiteturais de mitigação aplicáveis ao setor financeiro; o terceiro discute as práticas de conformidade, monitoramento contínuo e continuidade de negócios no contexto da regulação bancária brasileira. A terceira seção descreve a metodologia bibliográfica e documental adotada. A quarta seção apresenta e discute os resultados da análise. A quinta seção reúne as considerações finais, respondendo ao objetivo geral e indicando implicações para a gestão da segurança nos bancos brasileiros.

2 REFERENCIAL TEÓRICO

2.1 Arquiteturas de segurança em bancos brasileiros: Fundamentos normativos e técnicos

A segurança da informação nas instituições financeiras brasileiras é regulada por um conjunto normativo de múltiplas camadas que combina legislação federal, regulamentações do Banco Central do Brasil e padrões internacionais de gestão da segurança da informação. A Resolução n. 4.658, de 26 de abril de 2018, representa o marco regulatório central da segurança cibernética no sistema financeiro nacional, ao determinar que todas as instituições autorizadas pelo Banco Central implementem e

mantenham uma política de segurança cibernética baseada em princípios de confidencialidade, integridade, disponibilidade e autenticidade dos dados e sistemas. Semola (2014) sustenta que os princípios de confidencialidade, integridade e disponibilidade constituem a tríade fundamental sobre a qual toda arquitetura de segurança da informação deve ser construída, sendo que a violação de qualquer um desses princípios produz impactos que se propagam pelos demais, o que torna a abordagem integrada de proteção uma condição indispensável para a efetividade dos controles de segurança nas organizações contemporâneas.

A norma ABNT NBR ISO/IEC 27001:2022 estabelece os requisitos para implementação, manutenção e melhoria contínua de um Sistema de Gestão da Segurança da Informação (SGSI), oferecendo às instituições financeiras brasileiras um framework internacional reconhecido para a organização sistemática de seus controles de segurança. A adoção dessa norma pelo setor bancário brasileiro é fortemente recomendada pela regulação do Banco Central, que, embora não a imponha como obrigação formal explícita, orienta as instituições a adotarem padrões internacionais de segurança da informação compatíveis com os riscos de seu perfil operacional. Maldonado e Blum (2019) observam que a conformidade com a LGPD e com as regulamentações setoriais do Banco Central pode ser facilitada pela adoção de frameworks de segurança da informação como a ISO/IEC 27001, que organiza os controles de proteção em domínios abrangentes que cobrem as principais áreas de risco relevantes tanto para a proteção de dados pessoais quanto para a segurança cibernética mais ampla das instituições financeiras.

A Resolução n. 4.658/2018 do Banco Central do Brasil estabelece os elementos obrigatórios que a política de segurança cibernética das instituições financeiras deve conter:

> A política de segurança cibernética deve contemplar: I - os objetivos de segurança cibernética da instituicao; II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética; III - os controles específicos, incluindo os relacionados ao uso de tecnologias de autenticação e criptografia; IV - o registro, a análise da causa e do impacto, e o controle dos efeitos de incidentes relevantes para a instituição. (Banco Central do Brasil, 2018, art. 3).

O artigo 3 da Resolução n. 4.658/2018 deixa claro que a política de segurança cibernética deve ser um instrumento abrangente que articule objetivos estratégicos

com controles técnicos específicos e com mecanismos de registro e análise de incidentes, configurando uma arquitetura de segurança que integra as dimensões preventiva, detectiva e corretiva da proteção. Pinheiro (2021) destaca que a exigência de registro e análise de incidentes contida na resolução é especialmente significativa do ponto de vista da conformidade com a LGPD, pois o artigo 48 da lei impõe ao controlador o dever de comunicar à Autoridade Nacional de Proteção de Dados e ao titular os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, o que pressupõe a existência de sistemas de detecção e registro suficientemente sofisticados para identificar e documentar as violações de dados no momento em que ocorrem.

A gestão integrada de riscos nas instituições financeiras brasileiras tem seu enquadramento normativo principal na Resolução CMN n. 4.557, de 23 de fevereiro de 2017, que impõe a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos riscos operacionais, categoria que abrange diretamente os riscos cibernéticos associados às operações bancárias digitais. A aplicação da Resolução CMN n. 4.557/2017 ao contexto das ameaças cibernéticas exige que os bancos desenvolvam modelos de mensuração do risco cibernético compatíveis com os modelos de capital adotados pela organização, o que representa um desafio metodológico considerável, dada a dificuldade de quantificar probabilidades e impactos de ataques cibernéticos a partir de dados históricos limitados. Doneda (2019) argumenta que a prevenção de danos na era digital exige que as organizações adotem abordagens de risk management orientadas pela antecipação de ameaças emergentes e pelo fortalecimento das capacidades de detecção e resposta, em vez de se limitarem a reagir a incidentes já materializados.

A Resolução CMN n. 4.557/2017 define as obrigações de gerenciamento integrado de riscos aplicáveis às instituições financeiras, incluindo o risco operacional no qual se inserem as ameaças cibernéticas:

> As instituições referidas no art. 1o devem implementar estrutura de gerenciamento contínuo dos seguintes riscos: I - risco de crédito; II - risco de mercado; III - risco de liquidez; IV - risco operacional; V - risco de contraparte; VI - risco socioambiental, devendo ser observadas as diretrizes estabelecidas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil para cada uma dessas categorias de risco. (Banco Central do Brasil, 2017, art. 3).

A inserção do risco cibernético no âmbito do risco operacional, tal como determina a Resolução CMN n. 4.557/2017, tem implicações importantes para a arquitetura de segurança dos bancos brasileiros, pois significa que os controles de segurança cibernética precisam ser integrados às estruturas mais amplas de gestão de riscos operacionais das instituições, e não tratados como um domínio separado gerenciado exclusivamente pela área de tecnologia da informação. Semola (2014) enfatiza que uma das disfunções mais comuns nas organizações é a compartimentalização da gestão de segurança da informação em áreas técnicas isoladas, sem conexão com as estratégias corporativas de gestão de riscos, o que produz lacunas de visibilidade e de coordenação que comprometem a efetividade das medidas de proteção adotadas. A integração efetiva da segurança cibernética na estrutura de gestão de riscos corporativos dos bancos brasileiros representa, portanto, tanto um imperativo normativo quanto uma condição de efetividade das arquiteturas de segurança.

2.2 Ameaças cibernéticas no setor financeiro brasileiro: Categorias, vetores e modelos de mitigação

O panorama das ameaças cibernéticas que afetam os bancos brasileiros é caracterizado pela diversidade, pela sofisticação crescente e pela velocidade de evolução dos vetores de ataque utilizados por agentes maliciosos nacionais e internacionais. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) publica anualmente estatísticas detalhadas sobre os incidentes reportados ao centro, oferecendo um panorama quantitativo da evolução do ambiente de ameaças no país. De acordo com os dados do CERT.br (2022), o Brasil registrou volumes expressivos de tentativas de fraude, phishing, ataques distribuídos de negação de serviço (DDoS) e comprometimento de sistemas, com o setor financeiro figurando consistentemente entre os mais afetados em termos de impacto e frequência dos incidentes reportados. Semola (2014) observa que a natureza dos ativos que os bancos detêm, que inclui recursos financeiros diretamente manipuláveis por meios digitais, dados pessoais e financeiros de milhões de clientes e infraestruturas críticas de pagamento, torna as instituições financeiras alvos de altíssimo valor para praticamente todas as categorias de agentes de ameaça, desde oportunistas individuais até grupos criminosos organizados e, em alguns casos, agentes estatais.

As ameaças de ransomware direcionado a bancos e outras instituições financeiras representam uma das categorias de risco que mais cresceu em relevância na última metade da década anterior, combinando a capacidade de paralisação das operações com a extorsão financeira e o risco de exposição de dados sensíveis. Esse tipo de ataque explora vulnerabilidades em sistemas internos das instituições, frequentemente introduzidas por e-mails de phishing, comprometimento de credenciais de acesso privilegiado ou exploração de vulnerabilidades não corrigidas em softwares legados que ainda operam em muitos bancos brasileiros. Bioni (2021) destaca que a exposição de dados pessoais em incidentes de ransomware gera obrigações específicas de notificação à Autoridade Nacional de Proteção de Dados e aos titulares afetados, que as instituições precisam estar preparadas para cumprir dentro dos prazos estabelecidos pela LGPD e pelas regulamentações complementares da ANPD, o que pressupõe a existência de processos e sistemas de gestão de incidentes suficientemente maduros para identificar a extensão de uma violação de dados enquanto o incidente ainda está sendo contido.

A Pesquisa FEBRABAN de Tecnologia Bancária de 2022 dimensiona o esforço do setor bancário brasileiro em resposta ao crescimento das ameaças cibernéticas e evidencia o papel central da tecnologia nessa batalha:

> Os bancos brasileiros seguem ampliando os investimentos em segurança e proteção, com destaque para as iniciativas de inteligência artificial aplicadas à detecção de fraudes, sistemas de autenticação multifatorial e plataformas de resposta a incidentes. O setor financeiro nacional investe consistentemente em tecnologia de ponta para proteger seus clientes e suas infraestruturas, reconhecendo que a confiança dos usuários é o ativo mais valioso a ser preservado no ambiente financeiro digital. (Febraban, 2022, p. 38).

A constatação da FEBRABAN sobre a centralidade dos investimentos em detecção de fraudes e autenticação multifatorial reflete a evolução das prioridades arquiteturais de segurança dos bancos brasileiros, que progressivamente deslocaram o foco de defesas perimetrais para controles centrados na identidade e no comportamento dos usuários. Essa mudança de paradigma arquitetural expressa a adoção, ainda que parcial, do modelo de Zero Trust Architecture, que pressupõe que nenhum usuário, dispositivo ou rede deve ser automaticamente considerado confiável, mesmo dentro do perímetro da organização, e que cada acesso deve ser verificado de forma explícita com base em múltiplos fatores de autenticação e contexto. A norma ABNT NBR ISO/IEC 27001:2022 incorpora controles específicos que suportam a

implementação dessa abordagem arquitetural, incluindo exigências de gestão de identidades e acessos, de segmentação de redes e de monitoramento contínuo das atividades nos sistemas de informação (ABNT, 2022).

Os ataques de engenharia social direcionados aos clientes bancários representam outra categoria de ameaça que as arquiteturas de segurança dos bancos precisam endereçar, embora esse tipo de ataque explore primariamente vulnerabilidades humanas e não tecnológicas. O phishing, o vishing e as fraudes de SIM swap são técnicas que permitem a agentes maliciosos obter credenciais de acesso ou autorizar transações fraudulentas sem necessidade de comprometer diretamente os sistemas dos bancos, o que torna sua mitigação dependente de uma combinação de controles técnicos, como a verificação comportamental e a análise de anomalias em tempo real, e de investimentos em educação e conscientização dos clientes. Tepedino, Frazão e Oliva (2020) identificam que a responsabilidade civil dos bancos por danos decorrentes de fraudes que exploram dados pessoais obtidos de forma ilícita é um tema juridicamente complexo no contexto da LGPD, pois a lei estabelece um regime de responsabilidade que leva em consideração tanto as medidas de segurança adotadas pela instituição quanto o comportamento do próprio titular dos dados.

A ABNT NBR ISO/IEC 27001:2022 estabelece os princípios que devem orientar a construção de um sistema de gestão da segurança da informação capaz de responder ao ambiente dinâmico de ameaças cibernéticas:

> A organização deve determinar as questões externas e internas que são relevantes para seu proposito e que afetam sua capacidade de alcançar os resultados pretendidos de seu sistema de gestão da segurança da informação. Devem ser considerados os requisitos das partes interessadas relevantes, incluindo os requisitos legais, regulamentares e contratuais relacionados com a segurança da informação. (ABNT, 2022, item 4.1 e 4.2).

A exigência da norma ISO/IEC 27001:2022 de que a organização considere tanto o contexto externo quanto as partes interessadas relevantes na construção de seu sistema de gestão da segurança da informação é particularmente pertinente para os bancos brasileiros, que precisam harmonizar as exigências da regulação prudencial do Banco Central, os requisitos da LGPD, as expectativas de segurança dos clientes e os padrões internacionais de boas práticas em um único sistema coerente de gestão. Essa multiplicidade de requisitos não é necessariamente

contraditória, mas exige uma abordagem de conformidade integrada que identifique as sobreposições e as lacunas entre os diferentes conjuntos de exigências e as organize em uma arquitetura de controles unificada que atenda simultaneamente a todos os mandatos regulatórios e normativos aplicáveis. Maldonado e Blum (2019) ressaltam que a conformidade simultânea com a LGPD e com as normas de segurança cibernética do Banco Central é não apenas possível, mas necessária e potencialmente sinérgica, pois as duas estruturas normativas convergem na proteção dos dados dos clientes e na segurança dos sistemas que os processam.

2.3 Conformidade regulatória, monitoramento contínuo e continuidade de negócios

A conformidade regulatória no setor bancário brasileiro é um processo contínuo que demanda das instituições financeiras a capacidade de acompanhar e incorporar tempestivamente as mudanças em um ambiente normativo que está em permanente evolução. No campo específico da segurança cibernética, essa dinâmica é especialmente desafiadora porque o regulador bancário, o Banco Central do Brasil, tem emitido normas, circulares e orientações com crescente regularidade, refletindo a aceleração do ritmo de inovação tecnológica no setor financeiro e o correspondente aumento da complexidade e da diversidade das ameaças cibernéticas que os bancos precisam enfrentar. Semola (2014) argumenta que a conformidade regulatória, quando tratada pelas organizações como um objetivo em si mesmo, produz uma postura de segurança defensiva e retrospectiva que frequentemente se limita a atender o mínimo exigido pelas normas, sem desenvolver as capacidades proativas de gestão de riscos que são necessárias para enfrentar ameaças que ainda não foram capturadas pelo arcabouço regulatório existente.

O monitoramento contínuo das ameaças e das vulnerabilidades constitui uma das práticas mais críticas para a efetividade das arquiteturas de segurança bancária, pois é por meio desse monitoramento que as instituições conseguem detectar ataques em curso antes que produzam danos significativos e identificar vulnerabilidades em seus sistemas antes que sejam exploradas por agentes maliciosos. As plataformas de Security Information and Event Management (SIEM) e os centros de operações de segurança (SOCs) representam os instrumentos tecnológicos centrais do monitoramento contínuo nos bancos brasileiros de maior porte, integrando dados de

múltiplas fontes em um ambiente analítico que permite a correlação de eventos e a identificação de padrões anômalos indicativos de ataques. Doneda (2019) ressalta que o monitoramento contínuo, quando realizado com o rigor e a intencionalidade necessários, também contribui para o cumprimento das obrigações de proteção de dados impostas pela LGPD, pois permite a identificação precoce de violações de dados que demandam notificação às autoridades e aos titulares.

A Resolução n. 4.658/2018 impõe às instituições financeiras a obrigação de elaborar e manter um plano de ação e de resposta a incidentes que deve cobrir as principais dimensões da continuidade operacional:

> As instituições referidas no art. 1o devem elaborar plano de ação e de resposta a incidentes, a ser aprovado pelo conselho de administração ou, na sua ausência, pela diretoria da instituição, contemplando: I - as ações a serem realizadas antes, durante e após a ocorrência de incidentes; II - os procedimentos de escalonamento e de comunicação da ocorrência do incidente; III - as ações e procedimentos de retomada das atividades afetadas pelo incidente. (Banco Central do Brasil, 2018, art. 5).

O plano de ação e de resposta a incidentes exigido pelo artigo 5 da Resolução n. 4.658/2018 constitui o instrumento formal pelo qual a arquitetura de segurança dos bancos brasileiros incorpora a dimensão da continuidade de negócios, ao determinar que as instituições devem planejar antecipadamente não apenas como prevenir incidentes, mas como retomar as atividades afetadas quando os incidentes inevitavelmente ocorrem. Bioni (2021) observa que a exigência de continuidade operacional nos bancos deriva não apenas da regulação prudencial, mas também da natureza dos serviços financeiros como infraestrutura crítica da economia, cuja interrupção pode produzir efeitos sistêmicos que transcendem as fronteiras da instituição afetada e comprometem o funcionamento de todo o sistema financeiro. Essa dupla dimensão da continuidade de negócios, ao mesmo tempo obrigação regulatória e responsabilidade sistêmica, exige que os planos de continuidade dos bancos brasileiros sejam suficientemente robustos e testados para garantir a resiliência operacional mesmo nos cenários de ataques mais sofisticados e abrangentes.

A Pesquisa FEBRABAN de Tecnologia Bancária de 2022 registrou que os bancos brasileiros têm investido de forma significativa em modernização de suas infraestruturas de tecnologia da informação, com migração crescente para ambientes de computação em nuvem, adoção de arquiteturas de microsserviços e

implementação de práticas de DevSecOps que integram a segurança nos processos de desenvolvimento de software desde as fases iniciais do ciclo de vida. Essas transformações arquiteturais têm implicações diretas para a continuidade de negócios, pois alteram os padrões de falha dos sistemas e introduzem novos vetores de risco que os planos tradicionais de continuidade, concebidos para ambientes de tecnologia da informação mais homogêneos e controlados, frequentemente não contemplam de forma adequada. Pinheiro (2021) aponta que a migração para a computação em nuvem, amplamente adotada pelo setor bancário brasileiro, exige que os bancos revisem seus planos de continuidade de negócios para incorporar os riscos específicos dos ambientes em nuvem, incluindo a dependência de fornecedores externos, os riscos de indisponibilidade de serviços em nuvem e os desafios de portabilidade e recuperação de dados em cenários de falha de provedores.

A conformidade com a LGPD e com as normas de segurança cibernética do Banco Central exige que as instituições desenvolvam programas integrados de gestão que articulem as diferentes obrigações normativas em torno de uma estratégia coerente de proteção de dados e continuidade operacional. Tepedino, Frazão e Oliva (2020) sintetizam a essência dessa integração:

> A proteção de dados pessoais no ambiente financeiro digital nao pode ser concebida como um conjunto de controles isolados que respondem a mandatos regulatorios especificos, mas deve ser entendida como um sistema de governança que permeia toda a arquitetura organizacional e tecnológica da instituição, integrando as dimensões preventiva, detectiva e corretiva da segurança em um ciclo continuo de melhoria que acompanha a evolução do ambiente de ameaças e das exigências regulatórias. (Tepedino; Frazao; Oliva, 2020, p. 312).

A perspectiva de Tepedino, Frazão e Oliva sobre a integração das dimensões preventiva, detectiva e corretiva da segurança em um ciclo contínuo de melhoria captura com precisão o que a literatura de segurança da informação denomina modelo de maturidade de segurança cibernética, que avalia as organizações não apenas pela presença de controles técnicos específicos, mas pela sua capacidade de aprender continuamente com os incidentes ocorridos, adaptar suas defesas às ameaças emergentes e demonstrar de forma mensurável a evolução de suas capacidades de proteção ao longo do tempo. A norma ABNT NBR ISO/IEC 27001:2022, ao exigir a melhoria contínua do sistema de gestão da segurança da informação como um requisito formal, institucionaliza essa perspectiva evolutiva e a transforma em uma obrigação normativa que as instituições devem ser capazes de demonstrar em

auditorias e certificações (ABNT, 2022). Para os bancos brasileiros, a adoção de um modelo de maturidade de segurança cibernética que integre as exigências normativas nacionais com os padrões internacionais representa o caminho mais promissor para o desenvolvimento de arquiteturas de segurança verdadeiramente eficazes e resilientes.

3 METODOLOGIA

O presente estudo adota a pesquisa bibliográfica e documental como procedimento metodológico central, modalidade adequada para investigar fenômenos complexos que se situam na intersecção de diferentes campos disciplinares, como é o caso das arquiteturas de segurança cibernética em bancos brasileiros, tema que requer a articulação de conhecimentos provenientes da tecnologia da informação, do direito regulatório, da gestão de riscos e da ciência da administração. Gil (2010) define a pesquisa bibliográfica como aquela elaborada com base em material já publicado, constituído principalmente de livros, artigos de periódicos e, contemporaneamente, materiais disponibilizados na internet, modalidade que permite ao pesquisador construir uma síntese analítica a partir das contribuições de diferentes autores e perspectivas sobre o mesmo fenômeno. A pesquisa documental, que complementa a abordagem bibliográfica neste estudo, caracteriza-se pela análise de documentos que ainda não receberam tratamento analítico sistematizado, categoria em que se enquadram as resoluções normativas do Banco Central, os relatórios da FEBRABAN e os documentos técnicos do CERT.br.

O levantamento das fontes foi realizado por meio de buscas sistemáticas nas bases de dados SciELO, Portal de Periódicos da CAPES, Google Scholar, no sítio eletrônico do Banco Central do Brasil, no repositório da FEBRABAN e no portal do CERT.br. Foram utilizados os descritores "segurança cibernética em bancos", "arquitetura de segurança financeira", "ameaças cibernéticas setor financeiro", "continuidade de negócios em bancos", "conformidade regulatória LGPD bancos", "segurança da informação setor bancário" e "gestão de riscos cibernéticos", aplicados isoladamente e em combinações com os operadores booleanos AND e OR. Lakatos e Marconi (2017) orientam que o rigor na definição dos descritores e nos critérios de inclusão e exclusão das fontes é condição indispensável para a representatividade e a validade científica do corpus analítico de uma pesquisa bibliográfica, recomendação

que norteou de forma sistemática todos os procedimentos de busca adotados nesta pesquisa.

Os critérios de inclusão adotados para a composição do corpus analítico foram: (a) publicações em língua portuguesa, inglesa ou espanhola; (b) textos acadêmicos e técnicos publicados preferencialmente entre 2018 e 2025, admitindo-se obras clássicas de referência indispensáveis à fundamentação conceitual; (c) documentos normativos vigentes com relevância direta para o tema investigado; (d) relatórios institucionais de organismos de reconhecida idoneidade no campo da segurança cibernética e da tecnologia bancária; (e) disponibilidade integral do texto em formato eletrônico. Foram excluídos textos sem fundamentação teórica ou normativa explícita, artigos de opinião sem embasamento científico e materiais que não tratassem diretamente dos temas de segurança cibernética, conformidade regulatória ou continuidade de negócios no setor bancário. Severino (2017) esclarece que a pesquisa bibliográfica exige uma postura crítica e seletiva do pesquisador na avaliação das fontes, pois nem todo material publicado sobre um tema atende aos critérios de qualidade e pertinência necessários para fundamentar conclusões com rigor científico.

O corpus analítico resultante é composto por 16 obras e documentos, incluindo legislação federal, normativos do Banco Central do Brasil, norma técnica internacional (ABNT NBR ISO/IEC 27001:2022), relatório do CERT.br, pesquisa setorial da FEBRABAN e obras doutrinárias de referência sobre segurança da informação, proteção de dados e metodologia científica, conforme detalhado no Quadro 1. A composição do corpus buscou equilibrar a dimensão normativa, com a análise dos marcos regulatórios aplicáveis, a dimensão técnica, com a incorporação de padrões e frameworks de segurança reconhecidos internacionalmente, e a dimensão acadêmica e institucional, com obras e relatórios que contextualizam as práticas de segurança do setor bancário brasileiro no panorama mais amplo das ameaças e das boas práticas globais. Minayo (2014) orienta que a diversidade de perspectivas no corpus analítico de uma pesquisa qualitativa é um requisito metodológico que enriquece a análise ao expor o pesquisador a diferentes enquadramentos do mesmo fenômeno, estimulando o pensamento crítico e a produção de sínteses mais nuançadas e aprofundadas.

O procedimento analítico foi estruturado em três etapas. Na primeira etapa, exploratória, realizou-se a leitura integral de todos os textos e documentos normativos selecionados, com elaboração de fichamentos que registraram os conceitos centrais, as disposições normativas mais relevantes, os dados quantitativos citados e as referências cruzadas entre as diferentes fontes. Na segunda etapa, analítica, as contribuições das diferentes fontes foram organizadas em torno das três categorias temáticas que estruturam o referencial teórico: os fundamentos normativos e técnicos das arquiteturas de segurança bancária, as categorias de ameaças cibernéticas e os modelos de mitigação correspondentes, e as práticas de conformidade, monitoramento contínuo e continuidade de negócios. Na terceira etapa, sintética, as diferentes contribuições foram relacionadas entre si e confrontadas com os objetivos da pesquisa, produzindo a análise integrada que fundamenta os resultados e as considerações finais deste artigo.

As limitações inerentes à pesquisa bibliográfica e documental devem ser reconhecidas para a correta interpretação dos resultados. Em primeiro lugar, o corpus analítico, por mais representativo que seja, não esgota a totalidade da produção disponível sobre o tema, o que significa que perspectivas relevantes podem não estar adequadamente representadas nos resultados. Em segundo lugar, o dinamismo do ambiente regulatório e tecnológico da segurança cibernética bancária significa que novas ameaças, novos frameworks de segurança e novas regulamentações podem emergir após a conclusão da pesquisa, tornando alguns resultados parcialmente datados. Gil (2010) observa que a principal contribuição da pesquisa bibliográfica consiste na produção de sínteses teóricas e normativas que iluminam os debates em curso e oferecem subsídios para pesquisas empíricas e para a tomada de decisão prática, contribuição que este estudo pretende oferecer ao campo da segurança cibernética bancária no Brasil.

4 RESULTADOS E DISCUSSÃO

A análise do corpus bibliográfico e documental permitiu organizar os resultados em torno de quatro eixos temáticos que respondem diretamente aos objetivos da pesquisa: (a) o arcabouço normativo que regula a segurança cibernética nos bancos brasileiros e suas principais implicações para as arquiteturas de segurança; (b) as categorias de ameaças cibernéticas mais relevantes para o setor e os modelos arquiteturais de mitigação recomendados; (c) as práticas de monitoramento contínuo e sua relação com a conformidade regulatória; (d) os elementos essenciais dos planos de continuidade de negócios eficazes no setor bancário. Em relação ao primeiro eixo, os resultados confirmam que o setor bancário brasileiro opera sob um dos mais abrangentes arcabouços normativos de segurança cibernética do mundo, combinando a LGPD, a Resolução n. 4.658/2018 e a Resolução CMN n. 4.557/2017 em um conjunto de obrigações que cobre todas as principais dimensões da segurança da informação. Semola (2014) e Pinheiro (2021) convergem ao identificar que esse arcabouço normativo, embora robusto, impõe desafios de implementação que se intensificam nas instituições de médio e pequeno porte, que frequentemente não dispõem dos recursos técnicos e humanos necessários para traduzir as obrigações normativas em arquiteturas de segurança verdadeiramente eficazes.

Os resultados relativos ao segundo eixo temático, as ameaças cibernéticas e os modelos de mitigação, evidenciam que o ambiente de ameaças enfrentado pelos bancos brasileiros é multidimensional e exige respostas arquiteturais igualmente diversificadas. Os dados do CERT.br (2022) apontam para a crescente sofisticação dos ataques direcionados ao setor financeiro, com combinação de técnicas de engenharia social, exploração de vulnerabilidades técnicas e ataques a cadeias de fornecimento que tornam insuficientes as abordagens tradicionais de segurança perimetral. A adoção da norma ABNT NBR ISO/IEC 27001:2022 como framework de referência para a organização dos controles de segurança emerge da análise como uma das estratégias mais eficazes para estruturar arquiteturas de segurança abrangentes e auditáveis, pois a norma organiza os controles de segurança em domínios que cobrem sistematicamente as principais categorias de ameaças identificadas pela literatura e pelos relatórios setoriais (ABNT, 2022).

Um resultado de especial relevância diz respeito ao papel central do monitoramento contínuo nas arquiteturas de segurança dos bancos brasileiros contemporâneos. A análise da Resolução n. 4.658/2018 e das práticas descritas pela FEBRABAN (2022) revela que os bancos brasileiros de maior porte avançaram significativamente na implementação de capacidades de detecção e resposta a incidentes, investindo em plataformas de SIEM, em inteligência de ameaças e em equipes especializadas de SOC. Semola (2014) argumenta que o monitoramento contínuo é o componente da arquitetura de segurança que transforma a postura defensiva das organizações de reativa para proativa, ao permitir a identificação de ataques em estágios iniciais, antes que atinjam os sistemas mais críticos, o que reduz substancialmente o impacto potencial dos incidentes e o custo das ações de resposta e recuperação. Essa constatação é corroborada pelos dados da FEBRABAN (2022), que indicam que as instituições com maior maturidade em monitoramento contínuo apresentam tempos de detecção e contenção de incidentes significativamente menores do que aquelas que ainda dependem de detecção reativa.

Os resultados relativos à conformidade regulatória revelam uma tensão estrutural entre a natureza estática das normas e a natureza dinâmica das ameaças cibernéticas, que a literatura e os reguladores têm abordado por meio de regulações baseadas em princípios e em resultados, em vez de regras prescritivas e detalhadas. A Resolução n. 4.658/2018 exemplifica essa abordagem ao estabelecer os princípios e os objetivos da segurança cibernética bancária sem prescrever as soluções técnicas específicas a serem adotadas, deixando às instituições a responsabilidade de implementar os controles mais adequados ao seu perfil de risco. Maldonado e Blum (2019) e Doneda (2019) convergem ao identificar que essa abordagem regulatória baseada em resultados é mais eficaz para a proteção dos titulares de dados em ambientes de alta complexidade tecnológica, mas impõe às instituições a responsabilidade de demonstrar, de forma documentada e auditável, que os controles adotados são adequados e eficazes para os riscos de seu contexto operacional específico.

Os resultados relativos à continuidade de negócios evidenciam que os planos de continuidade dos bancos brasileiros estão passando por uma transformação significativa em resposta às mudanças nas arquiteturas tecnológicas adotadas pelo setor. A migração para ambientes de computação em nuvem, documentada pela

FEBRABAN (2022), introduz novos padrões de disponibilidade e de resiliência que superam em muitos aspectos as capacidades dos ambientes tradicionais de tecnologia da informação, mas também cria dependências de fornecedores externos que precisam ser gerenciadas de forma explícita nos planos de continuidade. Tepedino, Frazão e Oliva (2020) identificam que a responsabilidade dos bancos pela continuidade dos serviços financeiros digitais é, sob a perspectiva da LGPD, inseparável da responsabilidade pela proteção dos dados dos clientes, pois incidentes que comprometem a continuidade operacional frequentemente resultam também em exposição ou comprometimento de dados pessoais que geram obrigações adicionais de notificação e de reparação de danos.

Por fim, os resultados relativos ao papel da cultura organizacional de segurança na efetividade das arquiteturas de proteção cibernética dos bancos brasileiros revelam que os investimentos tecnológicos, por mais sofisticados que sejam, produzem resultados limitados quando não são acompanhados de transformações culturais que tornem a segurança uma responsabilidade compartilhada por todos os membros da organização. Semola (2014) e Bioni (2021) convergem nessa perspectiva ao identificar que as vulnerabilidades exploradas com maior frequência e sucesso pelos agentes de ameaça não são de natureza técnica, mas humana, envolvendo comportamentos inadequados de funcionários, falta de conscientização sobre ameaças de engenharia social e deficiências nos processos de gestão de acessos privilegiados. A norma ABNT NBR ISO/IEC 27001:2022 responde a essa realidade ao incluir entre os controles obrigatórios do sistema de gestão da segurança da informação exigências específicas de treinamento, conscientização e gestão de competências em segurança da informação, reconhecendo que a dimensão humana é tão relevante quanto a dimensão tecnológica para a efetividade das arquiteturas de segurança cibernética (ABNT, 2022).

5 CONSIDERAÇÕES FINAIS

O presente estudo permitiu construir uma compreensão integrada e aprofundada das arquiteturas de segurança adotadas por bancos brasileiros para a mitigação de ameaças cibernéticas, evidenciando que a efetividade dessas arquiteturas depende da articulação coerente entre as dimensões de conformidade regulatória, monitoramento contínuo e continuidade de negócios, que não podem ser tratadas de forma isolada sem comprometer a integridade do sistema de proteção como um todo.

Em relação ao objetivo geral do estudo, os resultados confirmam que as arquiteturas de segurança cibernética dos bancos brasileiros operam em um contexto normativo robusto e progressivamente mais exigente, composto pela Resolução n. 4.658/2018, pela Resolução CMN n. 4.557/2017 e pela LGPD, que em conjunto estabelecem obrigações abrangentes de segurança da informação, gestão de riscos e proteção de dados pessoais. A efetividade da conformidade com esse arcabouço normativo, contudo, não é garantida pela mera existência de políticas e controles formais, mas depende da qualidade da implementação, da adequação dos controles ao perfil de risco específico de cada instituição e da capacidade de demonstrar a efetividade dos controles de forma documentada e auditável.

No que se refere ao primeiro objetivo específico, sobre o arcabouço normativo da segurança cibernética bancária, os resultados confirmam que o ordenamento regulatório brasileiro para o setor financeiro é um dos mais abrangentes da América Latina, mas que a implementação efetiva das obrigações normativas enfrenta desafios significativos, especialmente nas instituições de médio e pequeno porte. A disparidade de maturidade em conformidade e em arquitetura de segurança entre os grandes bancos e as instituições menores é uma fragilidade sistêmica do ecossistema financeiro brasileiro, pois um elo fraco em qualquer ponto da cadeia de participantes pode comprometer a segurança do sistema como um todo, especialmente em ambientes de integração como o Open Finance.

Quanto ao segundo objetivo específico, relativo às categorias de ameaças cibernéticas e aos modelos de mitigação, os resultados evidenciam que a sofisticação crescente dos ataques direcionados ao setor financeiro exige que as arquiteturas de segurança dos bancos brasileiros evoluam de modelos baseados em defesa

perimetral para modelos baseados em zero trust e em monitoramento comportamental contínuo. A adoção da norma ABNT NBR ISO/IEC 27001:2022 como framework de referência para a organização dos controles de segurança emerge como uma das estratégias mais eficazes para estruturar arquiteturas abrangentes e auditáveis, pois a norma oferece uma linguagem comum e um conjunto sistemático de controles que facilita a demonstração de conformidade e a comunicação com reguladores e auditores.

Em relação ao terceiro objetivo específico, sobre as práticas de monitoramento contínuo e continuidade de negócios, os resultados apontam que os bancos brasileiros de maior porte avançaram de forma expressiva na implementação de capacidades de detecção e resposta a incidentes, mas que a maturidade dos planos de continuidade de negócios frequentemente não acompanha o ritmo das transformações tecnológicas. A migração para ambientes de computação em nuvem, que amplia significativamente a resiliência técnica dos sistemas bancários, introduz ao mesmo tempo novas dependências de fornecedores externos que precisam ser explicitamente incorporadas nos planos de continuidade para que a resiliência operacional seja mantida em cenários de falha de provedores críticos.

Uma das contribuições mais relevantes deste estudo para o debate acadêmico e prático sobre a segurança cibernética bancária no Brasil é a demonstração de que a fragmentação das responsabilidades de segurança entre áreas técnicas, jurídicas e de compliance, sem uma coordenação estratégica centralizada, é um dos principais determinantes da persistência de vulnerabilidades nas arquiteturas de segurança dos bancos brasileiros. A superação dessa fragmentação exige a construção de estruturas de governança de segurança com autoridade transversal, que posicionem a segurança cibernética como uma responsabilidade compartilhada por toda a organização e não como um domínio exclusivo das áreas técnicas.

Do ponto de vista das políticas públicas, os resultados indicam que o Banco Central do Brasil poderia ampliar a efetividade de seu arcabouço regulatório de segurança cibernética por meio de mecanismos que incentivem as instituições de menor porte a elevar seus padrões de conformidade, como programas de capacitação patrocinados pelo regulador, compartilhamento de informações sobre ameaças em

nível setorial e modelos simplificados de conformidade para instituições cujo perfil de risco não justifica os investimentos exigidos das grandes instituições. A criação de um programa de compartilhamento de inteligência sobre ameaças cibernéticas coordenado pelo Banco Central e pela FEBRABAN, à semelhança de iniciativas similares em outros países, seria uma iniciativa de alto impacto para a elevação do nível de segurança de todo o ecossistema financeiro brasileiro.

A relação entre a segurança cibernética dos bancos e a proteção dos direitos dos consumidores de serviços financeiros é outro aspecto que merece atenção das políticas públicas, pois os usuários de serviços bancários digitais são frequentemente os mais afetados pelos incidentes de segurança, na forma de fraudes, vazamentos de dados pessoais e indisponibilidade de serviços. A articulação entre a ANPD e o Banco Central na supervisão das práticas de segurança e proteção de dados no setor financeiro é, portanto, uma necessidade institucional que ainda está em construção no Brasil, sendo necessário que os dois reguladores desenvolvam mecanismos de cooperação e de coordenação que evitem lacunas e inconsistências na proteção dos titulares de dados que são simultaneamente clientes bancários.

As limitações deste estudo devem ser consideradas para a correta interpretação dos resultados apresentados. A natureza bibliográfica e documental da pesquisa não permite o acesso às práticas concretas de segurança implementadas pelas instituições financeiras brasileiras, dimensão que somente pesquisas empíricas de campo, com acesso a dados primários de auditorias, relatórios internos e entrevistas com gestores de segurança, poderiam captar com o nível de detalhe necessário para conclusões definitivas sobre a efetividade das arquiteturas de segurança adotadas. O dinamismo do ambiente regulatório e tecnológico da segurança cibernética bancária representa uma limitação adicional, pois novas resoluções do Banco Central, novos tipos de ataques e novas versões de frameworks de segurança podem modificar o quadro de referência analisado em prazo relativamente curto.

Pesquisas futuras poderiam contribuir de forma significativa para o avanço do conhecimento sobre o tema ao explorar as seguintes questões: a correlação entre o nível de maturidade em conformidade com a norma ISO/IEC 27001 e a exposição efetiva a incidentes cibernéticos nos bancos brasileiros; a efetividade dos planos de

continuidade de negócios dos bancos em cenários de ataques de ransomware sistêmicos que afetam múltiplas instituições simultaneamente; e o impacto da implementação do Open Finance sobre o perfil de risco cibernético dos bancos, especialmente das instituições menores que passam a integrar ecossistemas de compartilhamento de dados de maior complexidade e amplitude.

Conclui-se que o amadurecimento das arquiteturas de segurança cibernética no setor bancário brasileiro é um processo contínuo e inacabado, que exige das instituições financeiras, dos reguladores e da academia um compromisso permanente com a atualização dos conhecimentos, o aprimoramento das práticas e a produção de pesquisas que integrem as dimensões técnica, normativa e organizacional da segurança em análises que sejam ao mesmo tempo rigorosas e praticamente úteis para os gestores que precisam tomar decisões complexas em um ambiente de ameaças em permanente evolução. A proteção dos dados e dos recursos financeiros dos cidadãos brasileiros depende da qualidade dessas arquiteturas e da seriedade com que as instituições bancárias, os reguladores e a sociedade encaram os desafios da segurança cibernética no ambiente digital contemporâneo.

6 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2022. Segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação. Rio de Janeiro: ABNT, 2022.

BANCO CENTRAL DO BRASIL. Resolução CMN n. 4.557, de 23 de fevereiro de 2017. Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de capital. Diário Oficial da União, Brasília, 24 fev. 2017.

BANCO CENTRAL DO BRASIL. Resolução n. 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Diário Oficial da União, Brasília, 27 abr. 2018.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018.

CERT.br. Estatísticas dos Incidentes Reportados ao CERT.br. São Paulo: NIC.br, 2022. Disponível em: https://cert.br/stats/. Acesso em: 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, 2019.

FEDERAÇÃO BRASILEIRA DE BANCOS. Pesquisa FEBRABAN de Tecnologia Bancária 2022. São Paulo: FEBRABAN, 2022.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 5. ed. São Paulo: Atlas, 2010.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 8. ed. São Paulo: Atlas, 2017.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). LGPD: Lei Geral de Proteção de Dados Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MINAYO, Maria Cecília de Souza. O desafio do conhecimento: pesquisa qualitativa em saúde. 14. ed. São Paulo: Hucitec, 2014.

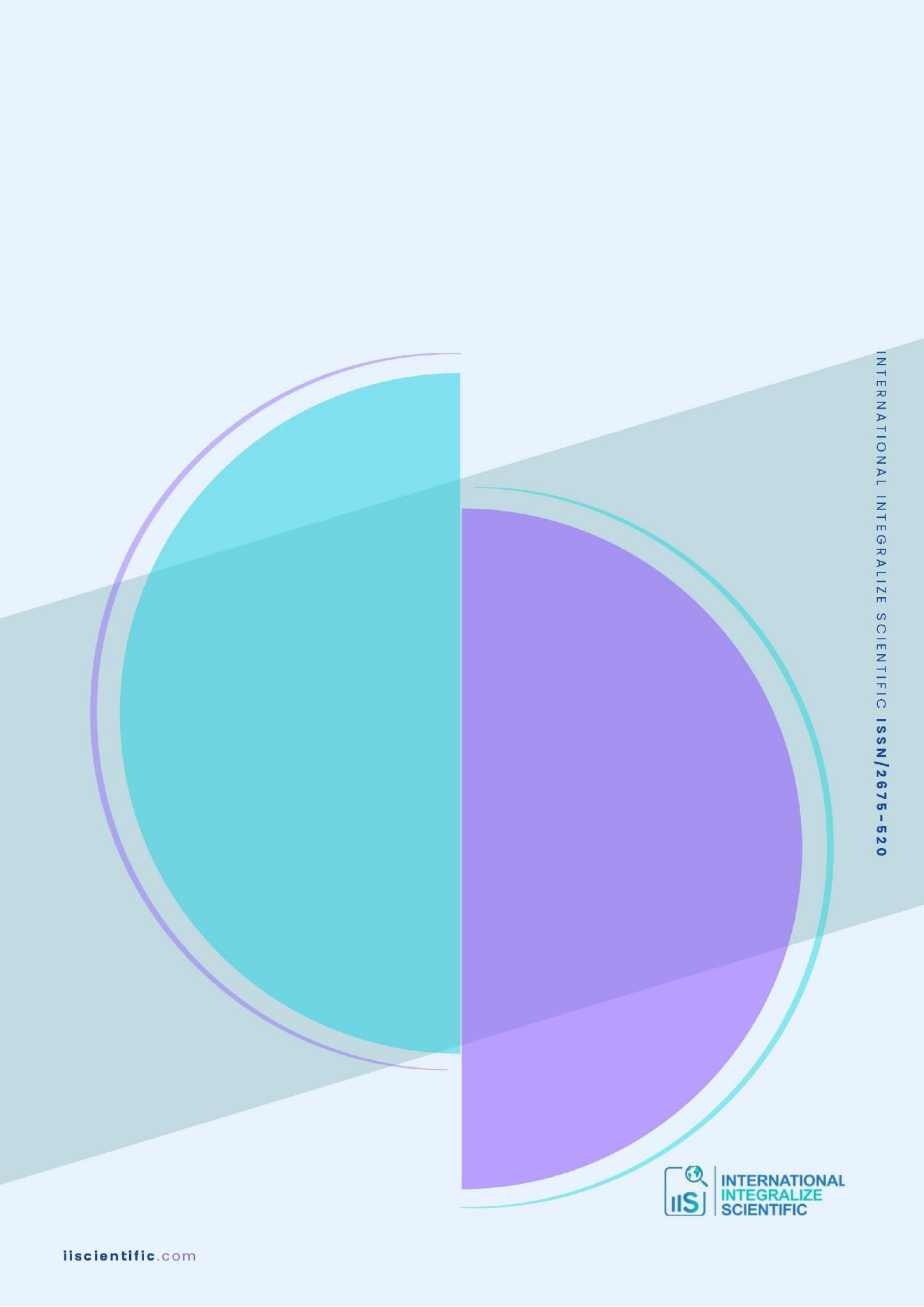
PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva, 2021.

SEMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. 2. ed. Rio de Janeiro: Campus/Elsevier, 2014.

SEVERINO, Antônio Joaquim. Metodologia do trabalho científico. 24. ed. São Paulo: Cortez, 2017.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

INTERNATIONAL INTEGRALIZE SCIENTIFIC ISSN/2675-520



INTERNATIONAL INTEGRALIZE SCIENTIFIC