UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador

2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador

2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador

2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador

2025

SUMÁRIO

Salvador

2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.

Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e

minimização.

A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.

A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.

Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.

Teixeira *et al*. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.

A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.

Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo' (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.

Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.

A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.

Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.

A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.

Nesse cenário, Teixeira *et al*. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.

A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.

Pil’ (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.

Salvador

2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados — comunicação clara, responsabilidade institucional e monitoramento constante — são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo’ (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais — conhecido internacionalmente como *Data Protection Officer (DPO)* — emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.

Pilo' (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.

Teixeira *et al*. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente — disponibilizar informações de forma controlada e auditável — pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.

Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.

Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro.

A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo’ (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa *et al*. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini *et al*. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.

Complementando essa discussão, Matos (2022) ressalta que o tratamento

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.

Prosseguindo nessa linha interpretativa, Souza *et al*. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.

Teixeira *et al*. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.

A discussão desenvolvida por Nascimento e D’Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva *et al*. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo *et al*. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda *et al*. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.

Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.

A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.

Em continuidade às análises sobre as implicações regulatórias, Souza *et al*. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.

Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um *framework (conjunto estruturado de diretrizes, princípios)* internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (*risk data aggregation*) e para a capacidade de reporte de informações (*risk reporting*) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.

O *framework* define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.

Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.

Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.

A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.

A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva *et al*., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.

No ambiente regulado pelo Bacen — especialmente após o Open Finance — as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.

No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.

Alves *et al*. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.

A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.

Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva *et al*., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.

Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.

As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.

Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva *et al*., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.

O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse

monitoramento ainda mais essencial.

Alves *et al*. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.

Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.

Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D’alkmin Neves

mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.

O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.

Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (*accountability*) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.

As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.

Alves *et al*. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.

Silva *et al*., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.

Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica.

Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.

Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza *et al*. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda *et al*., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D'alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D'alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda *et al*., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de "defesa em profundidade" converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza *et al*. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D'alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança.

Souza *et al*. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.

Por fim, as contribuições de Arruda *et al*., (2022) e Nascimento e D'alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini *et al*. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza *et al*. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes.

Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da “risk culture” no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.

Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa *et al*. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.

Pereira *et al*., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.

A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini *et al*. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.

Sousa *et al*. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-“Lava Jato”, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.

Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini *et al*. (2024), Freitas e Filho (2018), Sousa *et al*. (2024) e Pereira *et al*., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza *et al*. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento.

Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.

Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza *et al*. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.

Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.

A comunicação proativa após incidentes também é elemento chave da transparência. Sousa *et al*. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores.

Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini *et al*. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.

Souza *et al*. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.

Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza *et al*. (2024), Sousa *et al*. (2024) e

Rampini *et al*. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

Salvador

2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.

Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.

Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

Salvador

2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. **LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial**. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.

ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. **Journal of Health Informatics**, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.

ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. **Revista Ibérica de Sistemas e Tecnologias de Informação**, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.

BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. **Revista Ibmec de Direito**, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.

BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. **Em Questão**, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.

CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. **Revista Brasileira de Engenharia – Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência**, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.

DEPRÁ, C. **O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados**. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.

FARIAS, L.; OLIVEIRA, G. **Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD**. 2024. DOI: 10.5151/cidiconcic2023-107_645653.

Salvador

2025

FREITAS, C.; MAFFINI, M. **A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo**. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.

FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? **Cadernos Gestão Pública e Cidadania**, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.

IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. **CONTABILOMETRIA – Brazilian Journal of Quantitative Methods Applied to Accounting**, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.

MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.

MENDES, A.; JÚNIOR, V. **LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados**. 2024. DOI: 10.62140/amvj442024.

NASCIMENTO, E.; D'ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. **Revista Brasileira em Tecnologia da Informação**, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.

PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. **Revista Foco**, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.

PILO', F. **Segurança da informação no setor público e adequação à LGPD**. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.

RAMPINI, G. *et al*. **Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021**. Brazilian Applied Science Review, v. 8, n. 1, p. 130–147, 2024. DOI: 10.34115/basrv8n1-007.

SILVA, D.; FALCÃO, E. **Análise construtiva da Lei Geral de Proteção de Dados**.

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.

SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES – SBBD, 40., 2025, Fortaleza. *Proceedings of the 40th Brazilian Symposium on Data Bases*. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. *et al*. **A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período "Lava Jato"**. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. *et al*. **O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados**. Delos – Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. *et al*. **Proposta de um repositório digital para transparência de dados pessoais**. 2023. DOI: 10.5753/wide.2023.236108.

Salvador

2025

Relatório do Software Anti-plágio CopySpider
Para mais detalhes sobre o CopySpider, acesse:https://copyspider.com.br

Instruções
Este relatório apresenta na próxima página uma tabela com o resumo da análise do CopySpider. Cada linha associa o conteúdo do arquivo de entrada com um documento encontrado na internet (para "Busca em arquivos da internet") ou do arquivo de entrada com outros arquivos em seu computador (para "Pesquisa em arquivos locais").

A quantidade de termos comuns representa um fator utilizado no cálculo de similaridade dos arquivos. Quanto maior a quantidade de termos comuns, combinada com o agrupamento desses termos, maior a similaridade entre os arquivos.

No início de cada comparação entre arquivos, encontram-se um resumo numérico dos resultados:
- Arquivo 1: <nome do arquivo> (<Ni> termos)
- Arquivo 2: <nome do arquivo> (<Nc> termos)
- Termos comuns: <N>
- Similaridade:
  * Índice antigo (S): <x> %
  * Índice novo (Si): <y> %
  * Agrupamento (Sg): <Alto|Moderado|Baixo>

No texto do documento, os termos em comum são marcados em cores diferentes:
- Amarelo: quando são considerados no cálculo do Novo Índice de Semelhança (Si) e;
- Vermelho: quando estão agrupados e fazem parte do Índice de Agrupamento (Sg).

Os termos marcados em amarelo são comuns entre os documentos, mas, por não estarem agrupados, tendem a não caracterizar cópia. Os termos marcados em vermelho também são comuns e têm maior chance de serem interpretados como cópia.

É importante destacar que a classificação da semelhança como Alta, Moderada e Baixa não representa um "índice de plágio". Por exemplo, documentos que citam de forma direta (transcrição) outros documentos, podem ter uma similaridade Alta e ainda assim não podem ser caracterizados como plágio. Há sempre a necessidade do avaliador fazer uma análise para decidir se as semelhanças encontradas caracterizam ou não o problema de plágio ou mesmo de erro de formatação ou adequação às normas de referências bibliográficas.

Veja também:
Analisando o resultado do CopySpider
Qual o percentual aceitável para ser considerado plágio?
Como interpretar os índices de semelhança?

Versão do CopySpider: 3.5
Relatório gerado por: arthurlucas8@hotmail.com
Análise no modo: Web/Normal (disponibilidade de 99.17%) em 15:04 s
Idioma da busca: Português

Arquivos	Termos comuns	Semelhança	Agrupamento
TCC - ARTHUR LUCAS.pdf	163	Baixa	Moderado
X www.gov.br/transportes/pt-br/ouvidoria/perguntas-e-respostas-sob-aspectos-da-lgpd			
TCC - ARTHUR LUCAS.pdf	477	Baixa	Baixo
X portalantigo.ipea.gov.br/agencia/images/stories/PDFs/livros/livros/160719_governanca_ambiental.pdf			
TCC - ARTHUR LUCAS.pdf	476	Baixa	Baixo
X bibliotecadigital.enap.gov.br/bitstream/1/4281/1/5_Livro_Governança Gestão de Riscos e Integridade.pdf			
TCC - ARTHUR LUCAS.pdf	454	Baixa	Baixo
X bvsms.saude.gov.br/bvs/saudelegis/ans/2022/res0507_11_04_2022.html			
TCC - ARTHUR LUCAS.pdf	442	Baixa	Baixo
X repositorio.cgu.gov.br/bitstream/1/78223/1/Livro_Boas_Praticas_Regulatorias.pdf			
TCC - ARTHUR LUCAS.pdf	391	Baixa	Baixo
X www.mds.gov.br/webarquivos/publicacao/seguranca_alimentar/DHAA_SAN.pdf			
TCC - ARTHUR LUCAS.pdf	349	Baixa	Baixo
X repositorio.cgu.gov.br/bitstream/1/64869/11/Manual_PAD_2021_1.pdf			
TCC - ARTHUR LUCAS.pdf	300	Baixa	Baixo
X revistaft.com.br/o-direito-fundamental-a-protecao-de-dados-pessoais-no-brasil-desafios-e-perspectivas-para-a-efetivacao-da-lgpd			
TCC - ARTHUR LUCAS.pdf	292	Baixa	Baixo
X www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm			
TCC - ARTHUR LUCAS.pdf	282	Baixa	Baixo
X cfc.org.br/wp-content/uploads/2018/04/11_Guia_Normas_de_Auditoria_em_EPMP_volume_2_seminario-2.pdf			

Arquivos com problema de download

https://grupointercompany.com.br/2024/11/05/como-monitorar-e-gerenciar-vulnerabilidades-em-tempo-re

al - Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - curl: (6) Could not resolve host: grupointercompany.com.br; [csu] timeout

https://lupa.uol.com.br/jornalismo/2022/11/10/mensagem-saque-dinheiro - Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - curl: (6) Could not resolve host: lupa.uol.com.br

https://repositorio.ulisboa.pt/bitstreams/45f1d364-67b6-47bf-8712-40179831be05/download - Não foi possível baixar o arquivo. É recomendável baixar o arquivo manualmente e realizar a análise em conluio (Um contra todos). - Tipo do arquivo não identificado

Arquivos com problema de conversão

https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o CMN&numero=5267 - Não foi possível converter o arquivo. É recomendável converter o arquivo para texto manualmente e realizar a análise em conluio (Um contra todos).: msg.the_file_is_empty

https://www.mds.gov.br/webarquivos/publicacao/assistencia_social/cadernos/orientacoes-tecnicas-servicos-de-alcolhimento.pdf - Não foi possível converter o arquivo. É recomendável converter o arquivo para texto manualmente e realizar a análise em conluio (Um contra todos).: Erro ao tentar converter: Page tree root must be a dictionary

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: www.gov.br/transportes/pt-br/ouvidoria/perguntas-e-respostas-sob-aspectos-da-lgpd (5815 termos)
Termos comuns: 163
Similaridade
Índice antigo (S): 1,14%
Índice novo (Si): 1,90%
Agrupamento (Sg): Moderado
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 361eca0do20b21t21

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de

privacidade consolidada.
Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.
O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e
8

Salvador
2025

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.
A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada

operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior

relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança

estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que,

embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.

Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.

Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.

Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.

Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de

regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

Salvador
2025

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam

essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de

proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus

modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e

fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de
22

Salvador
2025

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de

segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados.

Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre

padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes
25

Salvador
2025

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais

cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança.
Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em

padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de

28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão

importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas

que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de 33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores.
Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que

stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à

responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em:

https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245.

Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato.

Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)

Arquivo 2: portalantigo.ipea.gov.br/agencia/images/stories/PDFs/livros/livros/160719_governanca_ambiental.pdf (103346 termos)

Termos comuns: 477

Similaridade

Índice antigo (S): 0,42%

Índice novo (Si): 5,58%

Agrupamento (Sg): Baixo

O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 55177c4co11b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador

2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e

capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade

de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.

Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e

Salvador
2025

minimização.

A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.

A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.

Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.

Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e

corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos

titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a

Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção

informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de

compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN.
Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.
A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e
18

Salvador
2025

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.
Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.
Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.
Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos

para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular

20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.
A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.
Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.
A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.
Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa
21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de
22

Salvador
2025

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há

mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de

segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.

Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.

Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.

As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.

Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois

cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade

jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador

2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

30

Salvador
2025

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin

neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal

a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios

estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.

Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.

Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da

consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health

Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e

Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA,

Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: bibliotecadigital.enap.gov.br/bitstream/1/4281/1/5_Livro_Governança Gestão de Riscos e Integridade.pdf (46624 termos)
Termos comuns: 476
Similaridade
Índice antigo (S): 0,86%
Índice novo (Si): 5,57%
Agrupamento (Sg): Baixo
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 6a577f37o13b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de

privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

Salvador
2025

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada

operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior

relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança

estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que,

embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de

regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

16

Salvador
2025

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam

essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de

proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus

modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e

fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de

segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados.

Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre

padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais

cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.

O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse

monitoramento ainda mais essencial.

Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.

Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.

Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em

padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.

O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam

27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.

Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.

As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.

Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.

Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de

28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão

importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas

que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores.
Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que

stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à

responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em:

https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245.

Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato.

Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: bvsms.saude.gov.br/bvs/saudelegis/ans/2022/res0507_11_04_2022.html (57518 termos)
Termos comuns: 454
Similaridade
Índice antigo (S): 0,69%
Índice novo (Si): 5,31%
Agrupamento (Sg): Baixo
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: fade5230o17b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

Salvador
2025

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.

Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.

A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador

2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ?

comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente

crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.

Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.

Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.

Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.

Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro.

A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e

responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das

informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam

políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.

Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.

A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.

Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.

Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado

de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação

dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem

regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança.

Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação

robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e

análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para

entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados

ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.

Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.

ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.

IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN

SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: repositorio.cgu.gov.br/bitstream/1/78223/1/Livro_Boas_Praticas_Regulatorias.pdf (66174 termos)
Termos comuns: 442
Similaridade
Índice antigo (S): 0,59%
Índice novo (Si): 5,17%
Agrupamento (Sg): Baixo
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 7fc6511ao11b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de

privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada

operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior

relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança

estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que,

embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de

regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam

essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de

proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

Salvador
2025

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus

modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e

fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de

segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados.

Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados. No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre

padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.

Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.

Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.

As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.

Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais

cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.

O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse

monitoramento ainda mais essencial.

Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.

Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.

Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em

padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.

O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam 27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.

Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.

As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.

Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.

Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de

28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão

importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas

que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores.
Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que

stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.

Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.

Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e

34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à

responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em:

https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245.

Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato.

Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: www.mds.gov.br/webarquivos/publicacao/seguranca_alimentar/DHAA_SAN.pdf (75514 termos)
Termos comuns: 391
Similaridade
Índice antigo (S): 0,46%
Índice novo (Si): 4,58%
Agrupamento (Sg): Baixo
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 0e5216e7o14b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de

privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada

operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior

relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança

estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que,

embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados
15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de

regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam

essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de

proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus

modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e

fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de
22

Salvador
2025

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de

segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados.

Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre

padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes
25

Salvador
2025

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais

cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.

O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse

monitoramento ainda mais essencial.

Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.

Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.

Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em

padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam

27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de

28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão

importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas

que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que

stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à

responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em:

https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245.

Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato.

Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)

Arquivo 2: repositorio.cgu.gov.br/bitstream/1/64869/11/Manual_PAD_2021_1.pdf (138305 termos)

Termos comuns: 349

Similaridade

Índice antigo (S): 0,23%

Índice novo (Si): 4,08%

Agrupamento (Sg): Baixo

O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: c503deeco13b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.
O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e
8

Salvador
2025

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.
A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.

Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.

A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador

2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ?

comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente

crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro.

A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e

responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das

informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam

políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.

Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.

A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.

Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.

Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado

de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação

dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem

regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes
25

Salvador
2025

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança.

Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos. Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação

robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e

análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para

entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.

Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.

Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.

A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados

ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.

Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.

ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.

IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN

SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)
Arquivo 2: revistaft.com.br/o-direito-fundamental-a-protecao-de-dados-pessoais-no-brasil-desafios-e-perspectivas-para-a-efetivacao-da-lgpd (5363 termos)
Termos comuns: 300
Similaridade
Índice antigo (S): 2,19%
Índice novo (Si): 3,51%
Agrupamento (Sg): Baixo
O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: a4f425c9o14b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador

2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e

capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade

de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e

corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos

titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a

Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados
15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção

informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de

compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos

para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular

20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de
22

Salvador
2025

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há

mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.

A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.

No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.

No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido

24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.

Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.

A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de

segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.

Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois

cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade

jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador

2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

30

Salvador
2025

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin

neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal

a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores.
Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios

estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.

Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.

Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e

34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da

consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health

Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e

Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA,

Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)

Arquivo 2: www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm (17733 termos)

Termos comuns: 292

Similaridade

Índice antigo (S): 1,11%

Índice novo (Si): 3,42%

Agrupamento (Sg): Baixo

O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 16eab198o10b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador
2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.
O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e
8

Salvador
2025

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.
A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.

Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.

A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador

2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ?

comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente

crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados

15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro.

A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e

responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

17

Salvador
2025

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das

informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam

políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular
20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.
A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.
Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.
A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.
Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa
21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.

Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.

A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.

Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.

Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado

de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação

dos princípios da LGPD.
A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.
No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados.
No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido
24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.
Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.
A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem

regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.
Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança.

Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação

robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.
O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam
27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.
Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.
As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.
Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.
Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador
2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e

análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para

entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados

ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.
Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.
Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e
34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.

Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.

ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.

IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA, Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN

SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.

==========

Arquivo 1: TCC - ARTHUR LUCAS.pdf (8537 termos)

Arquivo 2: cfc.org.br/wp-content/uploads/2018/04/11_Guia_Normas_de_Auditoria_em_EPMP_volume_2_seminario-2.pdf (63908 termos)

Termos comuns: 282

Similaridade

Índice antigo (S): 0,38%

Índice novo (Si): 3,30%

Agrupamento (Sg): Baixo

O texto abaixo é o conteúdo do documento **Arquivo 1**. Os termos em vermelho foram encontrados no documento **Arquivo 2**. Id: 804c2b84o8b0t0

==========

Salvador
2025

UNIVERSIDADE CATÓLICA DO SALVADOR

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Salvador
2025

ARTHUR LUCAS SANTOS GOMES

A APLICAÇÃO DA LGPD NAS INSTITUIÇÕES BANCÁRIAS: DESAFIOS DA PROTEÇÃO DE DADOS NO SETOR FINANCEIRO

Trabalho de Conclusão de Curso apresentado ao curso de Direito, da UNIVERSIDADE CATÓLICA DE SALVADOR, como requisito parcial para a Obtenção do grau de Bacharel em Direito.

Orientador: Humberto Teixeira

Salvador

2025

RESUMO

O presente trabalho tem como objetivo analisar a aplicação da Lei Geral de Proteção de Dados (LGPD) no setor bancário, avaliando os principais desafios enfrentados pelas instituições financeiras no cumprimento da legislação. Considerando que os bancos lidam diariamente com grandes volumes de informações sensíveis e estratégicas, a pesquisa investiga como a LGPD impacta as práticas de coleta, tratamento, armazenamento e compartilhamento de dados. Além disso, busca compreender as medidas de segurança adotadas, os riscos de sanções regulatórias e as implicações para a governança corporativa. O estudo traz a óptica de alguns autores e pretende, ainda, apontar as dificuldades práticas de adequação do setor e indicar possíveis soluções que promovam maior efetividade na proteção de dados no sistema financeiro brasileiro.

Palavras-chave: LGPD; conceitos; autores; bancário; desafios.

Salvador
2025

ABSTRACT

This paper aims to analyze the application of the General Data Protection Law (LGPD) in the banking sector, evaluating the main challenges faced by financial institutions in complying with the legislation. Considering that banks deal with large volumes of sensitive and strategic information daily, the research investigates how the LGPD impacts data collection, processing, storage, and sharing practices. Furthermore, it seeks to understand the security measures adopted, the risks of regulatory sanctions, and the implications for corporate governance. The study also aims to highlight the practical difficulties of compliance in the sector and suggest possible solutions that promote greater effectiveness in data protection in the Brazilian financial system.

Keywords: LGPD; concepts; authors; banking; challenges.

Salvador
2025

SUMÁRIO

7

Salvador
2025

1 INTRODUÇÃO

A aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) nas instituições bancárias representa um dos maiores desafios regulatórios da atualidade, pois o setor financeiro é responsável pelo tratamento contínuo e massivo de informações sensíveis, incluindo dados cadastrais, transacionais e comportamentais. A lei exige não apenas a adoção de medidas técnicas de segurança, mas também mudanças organizacionais profundas relacionadas à transparência, ao consentimento, ao controle de acesso e à governança de dados.

Nesse cenário, os bancos precisam conciliar inovação tecnológica, segurança cibernética e conformidade legal, especialmente em um ambiente marcado por constantes tentativas de fraude e ataques digitais. Além disso, a implementação da LGPD envolve a criação de políticas internas, revisão de fluxos informacionais e

capacitação permanente das equipes, o que reforça a necessidade de uma cultura de privacidade consolidada.

Diante desse contexto, surge a pergunta-problema: quais são os principais desafios enfrentados pelas instituições bancárias brasileiras para implementar, de forma efetiva, a LGPD na proteção dos dados pessoais de seus clientes ? parte-se da hipótese de que as maiores dificuldades decorrem da complexidade dos sistemas financeiros, da falta de integração entre plataformas tecnológicas, do elevado risco de incidentes cibernéticos e da ainda incipiente cultura organizacional voltada à governança de dados. Assim, busca-se compreender se esses fatores impactam diretamente a efetividade das ações de conformidade no setor.

O objetivo geral desta pesquisa é analisar os desafios da aplicação da LGPD nas instituições bancárias brasileiras. Para isso, foram definidos como objetivos específicos: identificar as exigências da LGPD que mais afetam o setor; examinar os entraves operacionais, jurídicos e tecnológicos enfrentados pelos bancos; e analisar as estratégias adotadas pelas instituições para aprimorar a segurança e a governança de dados. A realização deste estudo se justifica porque o setor financeiro possui forte impacto econômico e social, sendo responsável por informações extremamente sensíveis, cujo uso inadequado pode gerar danos significativos aos titulares e

comprometer a confiança no sistema bancário. Assim, discutir a adequação à LGPD contribui para o fortalecimento das práticas de compliance, segurança e gestão de riscos.

A metodologia utilizada baseou-se em uma revisão bibliográfica de caráter qualitativo, realizada por meio da consulta a artigos científicos, livros, relatórios técnicos, legislações, resoluções do Banco Central e documentos da Autoridade Nacional de Proteção de Dados (ANPD). Foram selecionadas publicações dos últimos dez anos disponíveis em bases como SciELO, Google Scholar, Periódicos CAPES e repositórios jurídicos especializados, priorizando estudos que discutem proteção de dados, segurança da informação e conformidade no setor financeiro. Após a seleção, o material foi analisado de forma interpretativa, permitindo identificar conceitos-chave, desafios recorrentes e estratégias institucionais relacionadas à aplicação da LGPD pelas instituições bancárias.

9

Salvador
2025

2 DESENVOLVIMENTO

2.1 LGPD, BASES LEGAIS E REQUISITOS PARA TRATAMENTO DE DADOS NO SETOR FINANCEIRO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, surgiu como marco regulatório brasileiro voltado à proteção da privacidade e ao uso responsável de informações pessoais. Inspirada especialmente no regulamento europeu GDPR, a LGPD ampliou a proteção de direitos fundamentais e introduziu regras aplicáveis a todos os setores da economia, com atenção especial ao setor financeiro, devido ao elevado volume de dados sensíveis tratados diariamente. No âmbito desse setor, a atuação do Banco Central do Brasil (Bacen) e do Conselho Monetário Nacional (CMN) é determinante para operacionalizar a lei, uma vez que cabe a tais órgãos detalhar diretrizes técnicas e procedimentos que garantam que bancos e instituições de pagamento atuem em conformidade com a legislação geral.

As bases legais previstas na LGPD constituem o núcleo estruturante da regulamentação do tratamento de dados em setores de alta sensibilidade, como o bancário. De acordo com Silva e Falcão (2024), a escolha adequada da base jurídica determina não apenas a legitimidade do tratamento, mas também a responsabilidade decorrente de sua utilização. No ambiente financeiro, a execução contratual e o legítimo interesse costumam ser predominantes, embora o consentimento permaneça possível em situações específicas. Essa pluralidade exige das instituições capacidade

de interpretar, aplicar e combinar bases legais de acordo com a natureza de cada operação.
Freitas e Maffini (2020) ressaltam que o crédito bancário intensifica a complexidade dessa escolha, pois envolve dados altamente sensíveis e perfis de risco que demandam análises automatizadas. Nesses casos, o consentimento pode ser considerado insuficiente ou inadequado, visto que o titular muitas vezes não compreende plenamente os impactos do compartilhamento. Assim, a execução contratual e o legítimo interesse tendem a assumir centralidade, embora devam ser acompanhados de salvaguardas capazes de garantir proporcionalidade e
10

Salvador
2025

minimização.
A discussão sobre dados sensíveis é igualmente relevante para o setor bancário, sobretudo quando se consideram informações que podem revelar vulnerabilidades financeiras ou perfis comportamentais. Almeida e Motta (2022) afirmam que o tratamento inadequado dessas informações coloca em risco a integridade e a reputação das instituições, exigindo estratégias rigorosas de limitação e anonimização. Em certa medida, essa preocupação se intensifica em contextos de open banking, em que a circulação de dados entre instituições amplia a superfície de risco.
A anonimização, embora apresentada pela LGPD como mecanismo de mitigação, não elimina por completo a possibilidade de reidentificação, especialmente em sistemas dotados de grandes volumes de dados e cruzamentos complexos. Mendes e Júnior (2024) alertam que tecnologias avançadas de mineração de dados podem reconstruir perfis mesmo após processos de anonimização, o que exige mecanismos adicionais de proteção. Dessa forma, o setor bancário deve adotar critérios mais robustos que garantam irreversibilidade prática e jurídica.
Transparência e clareza comunicativa figuram como eixos essenciais para a conformidade, especialmente porque a LGPD estabelece o dever de informar de forma acessível e compreensível. Farias e Oliveira (2024) destacam que a linguagem utilizada pelas instituições muitas vezes se mostra técnica demais, dificultando que os titulares compreendam a extensão do tratamento. Assim, o design da informação surge como ferramenta estratégica para tornar políticas de privacidade menos opacas e mais alinhadas ao entendimento do consumidor.
Teixeira et al. (2023) argumentam que a transparência não depende apenas da clareza textual, mas também de mecanismos tecnológicos que permitam ao titular acessar suas informações e acompanhar sua utilização. Repositórios digitais e painéis de controle, por exemplo, podem ampliar o senso de autonomia e

corresponsabilidade. No setor bancário, esses instrumentos ganham ainda maior relevância devido ao volume de operações realizadas diariamente.
A LGPD também impõe às instituições o dever de documentar suas decisões jurídicas, técnicas e administrativas relacionadas ao tratamento de dados. Segundo
11

Salvador
2025

Almeida e Motta (2022), essa documentação não é apenas um requisito formal, mas uma forma de demonstrar accountability diante de órgãos fiscalizadores. No setor bancário, essa prática funciona como mecanismo de rastreabilidade, essencial em auditorias e processos de due diligence.
Por fim, cabe reconhecer que o cumprimento das bases legais e dos requisitos formais só se efetiva quando integrado a uma cultura organizacional de proteção de dados, conforme destaca Pilo? (2025). Isso implica compreender que a conformidade não deve ser limitada à implementação mecânica de normas, mas inserir-se em práticas contínuas de gestão, monitoramento e revisão. Dessa forma, o setor bancário se aproxima de um modelo de governança mais maduro, sensível às dinâmicas regulatórias e tecnológicas contemporâneas.

2.1.1 Direitos dos titulares e adaptações no atendimento bancário

A consolidação dos direitos dos titulares na LGPD representa uma mudança paradigmática em setores que tradicionalmente operavam sob lógica verticalizada de gestão de dados, como o bancário. Silva e Falcão (2024) salientam que tais direitos reconfiguram a relação entre instituição e cliente, reforçando o papel do titular como agente ativo no ciclo informacional. Esse reposicionamento exige que os bancos revisem fluxos operacionais, documentos internos e práticas de atendimento.
Dentre esses direitos, portabilidade, acesso e correção assumem grande relevância. Conforme Freitas e Maffini (2020), a portabilidade, ao permitir a migração de dados entre instituições, fortalece a competição e reduz assimetrias informacionais. Entretanto, sua implementação não é trivial, pois envolve padrões de interoperabilidade que o setor bancário ainda busca consolidar. A interoperabilidade segundo a própria secretaria de Governo Digital (SGD-Brasil), pode ser compreendida como a capacidade de diferentes sistemas, plataformas ou organizações compartilharem informações de maneira integrada, segura e eficiente, permitindo que dados circulem entre ambientes tecnológicos distintos sem perda de significado ou funcionalidade. Para alguns autores, esse conceito envolve tanto padrões técnicos de compatibilidade quanto requisitos organizacionais e jurídicos que asseguram a
12

Salvador
2025

comunicação entre sistemas heterogêneos, promovendo cooperação e continuidade operacional.
A correção, por sua vez, demanda mecanismos ágeis para atualização, evitando prejuízos ao consumidor.
Farias e Oliveira (2024) mostram que a compreensão desses direitos depende da forma como são comunicados. Políticas extensas, tecnicamente complexas e fragmentadas geram obstáculos à compreensão. No contexto bancário, esse problema é ainda mais evidente, dada a natureza técnica dos produtos financeiros. Assim, o aprimoramento do design informacional é fundamental para garantir efetividade e não apenas formalidade.
A adequação aos prazos de resposta é igualmente desafiadora. Mendes e Júnior (2024) observam que instituições que lidam com alto volume de demandas enfrentam dificuldades para responder de forma tempestiva, especialmente diante de solicitações que envolvem múltiplos sistemas internos. Contudo, o não atendimento dentro dos prazos pode ser interpretado como violação de direitos, gerando risco regulatório.
Nesse cenário, Teixeira et al. (2023) defendem a criação de repositórios digitais e soluções automatizadas para facilitar o atendimento das solicitações dos titulares. Esses mecanismos reduzem tempo de resposta e promovem maior rastreabilidade das interações. No setor bancário, tais soluções tendem a ser essenciais, considerando o fluxo constante de consultas e pedidos.
A criação de canais especializados em privacidade constitui outra demanda da LGPD. Almeida e Motta (2022) pontuam que o atendimento deve ser separado dos canais tradicionais, evitando que dúvidas sobre privacidade sejam tratadas como demandas comuns. Essa abordagem melhora a qualidade da resposta e demonstra compromisso institucional com a proteção de dados.
Pil? (2025), ao analisar práticas de segurança informacional, afirma que a interação entre atendimento e governança deve ser contínua, já que dúvidas dos titulares podem revelar vulnerabilidades não mapeadas. Assim, reclamações e pedidos repetidos devem ser vistos como indicadores de falhas nos processos internos de comunicação, transparência ou segurança.
13

Salvador
2025

Deprá (2025) evidencia que a compreensão e o atendimento aos direitos dos

titulares só se concretizam plenamente quando acompanhados de governança estruturada. Embora seu estudo trate do setor público, os princípios analisados ? comunicação clara, responsabilidade institucional e monitoramento constante ? são plenamente aplicáveis às instituições bancárias. Isso reforça que o respeito aos direitos do titular integra um sistema mais amplo de governança de dados.

2.1.2 Obrigações de segurança e governança impostas aos bancos

A segurança da informação ocupa posição estratégica na adequação bancária à LGPD, sobretudo diante da natureza sensível das informações tratadas. Mendes e Júnior (2024) sustentam que os vazamentos recentes evidenciam fragilidades estruturais que não podem ser ignoradas. Em instituições financeiras, tais incidentes não afetam apenas indivíduos, mas a estabilidade e a confiança do sistema como um todo.

Os Relatórios de Impacto à Proteção de Dados (RIPD) constituem instrumentos centrais para essa governança. Almeida e Motta (2022) explicam que tais relatórios permitem identificar riscos, antecipar cenários e implementar medidas de mitigação, funcionando como mecanismo preventivo. No setor bancário, sua utilidade é ampliada devido ao contínuo surgimento de novos produtos digitais e modelos analíticos baseados em big data.

As exigências de registro de operações de tratamento, por sua vez, consolidam práticas de accountability. Segundo Silva e Falcão (2024), o registro detalhado das operações confere rastreabilidade e transparência, permitindo identificar eventuais desvios ou acessos indevidos. Para bancos, essa rastreabilidade é fundamental não apenas para fins regulatórios, mas também para auditorias internas e investigações de fraude.

O controle interno de acesso está diretamente relacionado à necessidade de garantir que apenas profissionais autorizados manipulem informações sensíveis. Pilo? (2025) destaca que a lógica de privilégio mínimo, se corretamente aplicada, reduz falhas humanas e limita a circulação de dados. Tal abordagem se mostra essencial

em sistemas bancários complexos, onde o número de usuários internos tende a ser elevado.

A figura do Encarregado pelo Tratamento de Dados Pessoais ? conhecido internacionalmente como Data Protection Officer (DPO) ? emerge como eixo articulador da governança de dados. Trata-se do profissional designado pela instituição para atuar como canal de comunicação entre o controlador, os titulares e a

Autoridade Nacional de Proteção de Dados (ANPD). Deprá (2025) argumenta que, embora sua análise se concentre no setor público, o papel do DPO é igualmente crucial no ambiente bancário, pois envolve comunicação com titulares, articulação institucional e monitoramento contínuo. Em instituições financeiras, esse papel se expande devido à complexidade regulatória e tecnológica.
Pilo? (2025) acrescenta que a segurança da informação não deve ser encarada como mera obrigação legal, mas como valor organizacional capaz de orientar decisões estratégicas. A adoção de protocolos de segurança, testes de vulnerabilidade e auditorias periódicas fortalece a resiliência institucional e reduz danos potenciais. Para os bancos, tais práticas também protegem sua imagem e competitividade.
Teixeira et al. (2023) apontam que mecanismos de transparência também integram a governança, permitindo ao titular verificar a utilização de suas informações. Embora seu estudo trate de repositórios de dados pessoais, a lógica subjacente ? disponibilizar informações de forma controlada e auditável ? pode ser facilmente estendida ao setor bancário. Assim, transparência e segurança passam a caminhar juntas.
Mendes e Júnior (2024) ressaltam que a efetividade da segurança depende de fatores humanos, organizacionais e culturais. Normas e tecnologias são insuficientes se não acompanhadas de práticas educativas e monitoramento constante. Assim, o setor bancário deve combinar mecanismos técnicos, políticas robustas e cultura institucional orientada à proteção de dados, consolidando uma governança coerente e abrangente.

2.1.3 Regulamentação do Bacen e do CMN sobre proteção de dados
15

Salvador
2025

A regulação exercida pelo Banco Central do Brasil (Bacen) e pelo Conselho Monetário Nacional (CMN) torna-se decisiva porque ambos são responsáveis pela normatização e supervisão das atividades financeiras. Assim, embora a LGPD seja uma lei geral aplicável a todos os setores, cabe ao Bacen detalhar sua aplicação prática no sistema financeiro, definindo requisitos técnicos, padrões de segurança e obrigações de governança que asseguram que bancos, cooperativas e instituições de pagamento tratem dados pessoais em conformidade com o marco legal.
Conforme analisa Beltrao (2025), a implementação da LGPD no setor bancário requer mecanismos de controle e consentimento mais rigorosos, orientados por normas infraconstitucionais que disciplinam o uso de dados. Assim, a proteção

informacional, embora estabelecida por lei federal, ganha efetividade por meio de regulamentações específicas que moldam as práticas internas do sistema financeiro. A abordagem das normas do Banco Central é fundamental, pois se trata de normas infraconstitucionais que concretizam, no setor financeiro, princípios e obrigações estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Enquanto a LGPD estabelece diretrizes gerais para o tratamento de dados pessoais, as regulamentações do Bacen detalham como essas diretrizes devem ser aplicadas na prática pelas instituições financeiras, dada a natureza sensível e estratégica dos dados envolvidos.

Nesse contexto, a Resolução Bacen nº 4.658/2018 desempenha papel central ao instituir requisitos mínimos de segurança cibernética, governança e controle no processamento e armazenamento de dados, inclusive em serviços de computação em nuvem. Ao exigir que as instituições mantenham políticas formais de segurança, gestão de riscos, planos de resposta a incidentes e mecanismos de mitigação voltados à proteção da informação, a norma complementa diretamente os princípios de segurança, prevenção e responsabilização previstos na LGPD. Assim, funciona como ponte entre a legislação geral e as necessidades operacionais específicas do sistema financeiro.

De igual modo, a Resolução BCB nº 1/2020, que disciplina o Sistema Financeiro Aberto (Open Banking), reforça a importância da interoperabilidade segura

ao regulamentar o compartilhamento padronizado de dados e serviços entre instituições participantes. A norma determina requisitos técnicos, padrões de comunicação, consentimento qualificado e governança compartilhada, assegurando que a circulação de dados ocorra de forma estruturada, transparente e compatível com a LGPD. Dessa forma, estabelece salvaguardas que viabilizam a inovação no mercado bancário sem violar os direitos dos titulares.

Em síntese, tanto a Resolução nº 4.658/2018 quanto a Resolução BCB nº 1/2020 atuam como mecanismos de aplicação prática da LGPD no âmbito financeiro, delineando parâmetros técnicos, organizacionais e jurídicos que permitem a conformidade das instituições. Ao disciplinarem segurança, interoperabilidade e compartilhamento de dados, essas normas fortalecem a proteção do titular e reduzem assimetrias regulatórias, promovendo maior segurança jurídica e confiança no ecossistema bancário.

Nesse mesmo percurso interpretativo, Almeida e Motta (2022) explicam que a LGPD introduz mudanças profundas nas rotinas de conformidade, impondo às instituições financeiras a revisão de políticas internas e dos fluxos de

compartilhamento de informações. As diretrizes editadas pelo Bacen complementam essa adaptação ao detalhar obrigações voltadas à segurança, prevenção e responsabilização, exigindo governança compatível com os princípios legais. Com isso, os bancos passam a adotar mecanismos capazes de assegurar integridade, rastreabilidade e coerência na gestão de dados pessoais.

A partir da discussão apresentada por Freitas e Maffini (2020), torna-se evidente que o tratamento de informações no crédito bancário requer precisão, transparência e definição clara de finalidade. O Bacen e o CMN fortalecem esses parâmetros ao regulamentar o uso do cadastro positivo e estabelecer requisitos técnicos alinhados à LGPD. Essa articulação reforça que as operações financeiras, por envolverem dados estratégicos e sensíveis, demandam cuidados ampliados, garantindo proteção compatível com a relevância social e econômica das informações tratadas.

Seguindo essa lógica de fortalecimento institucional, Deprá (2025) observa que a governança de dados depende da atuação de profissionais especializados

responsáveis por orientar e fiscalizar o tratamento de informações. A figura do encarregado, prevista pela LGPD, ganha papel central no setor bancário ao promover a harmonização entre práticas administrativas e regulamentações específicas do Bacen. Dessa forma, a supervisão interna torna-se elo essencial entre a legislação geral e as normas setoriais, contribuindo para a mitigação de riscos e o aprimoramento da gestão informacional.

A análise desenvolvida por Silva e Falcão (2024) demonstra que a amplitude da LGPD alcança todas as operações de tratamento realizadas no país, abrangendo diretamente as atividades financeiras. Ao atuarem como controladoras de dados, as instituições bancárias precisam observar princípios como necessidade, adequação e prevenção. As resoluções do Bacen e do CMN complementam esse conjunto normativo ao estabelecer medidas concretas que assegurem continuidade operacional, proteção técnica e responsabilidade diante dos titulares.

Prosseguindo com essa articulação normativa, Mendes e Júnior (2024) enfatizam que a eficácia da LGPD depende da capacidade das instituições de prevenir incidentes que comprometam a confiança pública, realidade particularmente sensível no setor bancário. As diretrizes emitidas pelo Bacen reforçam essa obrigação ao exigir auditorias constantes, monitoramento permanente e planos de contingência capazes de reduzir impactos. Dessa integração entre legislação geral e regulação financeira emerge um ambiente em que a segurança dos dados passa a ser componente estruturante da estabilidade do sistema.

Como observa Pilo? (2025), a conformidade com a LGPD exige mecanismos de proteção que assegurem confidencialidade, integridade e disponibilidade das informações tratadas. No contexto bancário, tais requisitos adquirem peso ainda maior devido ao volume e à sensibilidade dos registros armazenados, o que demanda observância simultânea à legislação federal e às resoluções do Bacen e do CMN. Essa convergência demonstra que a governança de dados não se limita ao cumprimento formal de normas, mas constitui dimensão essencial para a operação e a credibilidade das instituições financeiras.

A análise desenvolvida por Sousa et al. (2024) evidencia que as práticas de compliance no setor financeiro passaram a incorporar medidas de transparência e

responsabilização que dialogam diretamente com as exigências da LGPD. As resoluções emitidas pelo Bacen reforçam essa transformação ao definir padrões de governança para o tratamento de dados, impondo controles mais rigorosos sobre comunicação e monitoramento das operações. Assim, a proteção informacional deixa de ser apenas obrigação normativa para se consolidar como elemento estratégico na estrutura de conformidade das instituições financeiras.

Dando continuidade a essa compreensão ampliada, Rampini et al. (2024) observam que a gestão de riscos assume dimensão ainda mais abrangente após a vigência da LGPD, especialmente em ambientes regulados como o sistema bancário. As determinações do Bacen e do CMN vinculam a governança de dados a modelos metodológicos capazes de identificar vulnerabilidades e acompanhar fluxos informacionais. Essa convergência entre legislação geral e regulação setorial fortalece a previsibilidade das operações e garante maior segurança jurídica no processamento de dados pessoais.

Nessa mesma direção, Pereira, Silva e Pinto (2025) destacam que a atuação da auditoria interna torna-se componente fundamental para o fortalecimento da transparência corporativa, sobretudo em instituições sujeitas à supervisão constante. A LGPD intensifica essa responsabilidade ao exigir rastreabilidade e controle contínuo sobre o ciclo de tratamento de dados, ampliando a necessidade de verificação sistemática. As resoluções do Bacen complementam esse cenário ao estabelecer parâmetros objetivos para monitoramento e conformidade, reforçando a proteção do titular e a credibilidade das instituições.

Sob outro enfoque, Freitas e Fontes Filho (2018) apontam que a governança corporativa no setor bancário depende da implementação de mecanismos que assegurem responsabilidade, supervisão e controle sobre informações estratégicas. A LGPD agrega novos requisitos a essa estrutura ao determinar princípios específicos

para o tratamento de dados pessoais, obrigando as instituições a ajustar seus modelos internos. Paralelamente, as diretrizes do Bacen e do CMN disciplinam políticas de risco operacional e continuidade de negócios, promovendo alinhamento entre práticas internas e exigências contemporâneas de governança.
Complementando essa discussão, Matos (2022) ressalta que o tratamento
19

Salvador
2025

adequado de informações pessoais demanda clareza e rigor, principalmente quando envolve serviços amplamente utilizados pela sociedade. No sistema bancário, tais cuidados tornam-se mais complexos pela natureza sensível dos dados tratados e pelo volume de usuários atendidos. As normas do Bacen, ao regulamentarem incidentes de segurança e comunicações obrigatórias, reforçam a necessidade de aderência aos princípios da LGPD, fortalecendo a segurança jurídica e tecnológica que orienta a relação com os titulares.
Prosseguindo nessa linha interpretativa, Souza et al. (2024) indicam que a expansão das tecnologias digitais modifica significativamente a dinâmica entre instituições financeiras e titulares de dados, exigindo governança flexível e atualizada. A LGPD estabelece parâmetros essenciais para coleta, uso e armazenamento de informações, enquanto o Bacen detalha responsabilidades operacionais que vinculam o setor às melhores práticas de proteção. Esse alinhamento entre inovação tecnológica e regulação garante maior confiabilidade e antecipa riscos associados ao tratamento informacional.
Teixeira et al. (2023) observam que a transparência no tratamento de dados pressupõe o uso de instrumentos capazes de evidenciar e documentar todas as etapas do ciclo informacional. No setor bancário, essa necessidade é intensificada pela complexidade dos fluxos e pela obrigação de assegurar segurança integral das operações. As resoluções do Bacen e do CMN, ao definirem padrões de registro e documentação, favorecem a rastreabilidade exigida pela LGPD, ampliando a confiança dos titulares nas instituições responsáveis pelo tratamento.
A discussão desenvolvida por Nascimento e D?Alkmin Neves (2025) evidencia que a segurança da informação constitui fundamento indispensável para o cumprimento das normas regulatórias no setor financeiro, sobretudo após a consolidação da LGPD. A definição de controles rigorosos de acesso, autenticação contínua e prevenção de incidentes, conforme orienta o Bacen, eleva os padrões de confiabilidade das operações bancárias. Nesse contexto, a arquitetura Zero Trust (estrutura de segurança que exige que todos os usuários, dentro ou fora da rede da organização, sejam continuamente autenticados, autorizados e validados antes de receberem acesso aos aplicativos e dados da rede) ganha relevância ao articular

20

Salvador
2025

práticas tecnológicas e mecanismos de governança, reforçando que a proteção de dados deve integrar tanto a estrutura técnica quanto os processos gerenciais das instituições.

A esse entendimento soma-se a análise de Silva et al. (2025), que reconhecem na rastreabilidade dos dados um componente essencial da governança informacional. A LGPD exige documentação precisa que permita verificar o ciclo completo de tratamento, exigência que se harmoniza com as resoluções do Bacen voltadas ao registro e monitoramento das operações. Ao estabelecer parâmetros claros, o órgão regulador assegura que os bancos desenvolvam sistemas capazes de garantir transparência e confiabilidade no uso das informações, fortalecendo a aderência ao marco legal vigente.

Nesse mesmo eixo interpretativo, Carmo et al. (2021) ressaltam que a identificação de vulnerabilidades tecnológicas é condição indispensável para reduzir riscos em ambientes fortemente dependentes de infraestrutura digital. A LGPD reforça essa necessidade ao exigir medidas que atenuem eventuais falhas, enquanto o Bacen determina padrões específicos de resposta e mitigação aplicáveis ao setor bancário. Essa interação normativa amplia a resiliência institucional e favorece práticas preventivas alinhadas às expectativas regulatórias, fortalecendo a continuidade das operações financeiras.

A leitura de Brandt e Vidotti (2024) contribui ao demonstrar que a organização coerente das informações é determinante para a eficiência de sistemas complexos, especialmente quando envolvem bases amplas e heterogêneas. No âmbito financeiro, essa organização deve observar princípios da LGPD, como clareza e adequação, associados às diretrizes do Bacen e do CMN relativas à classificação e ao controle dos dados. A junção dessas exigências aprimora a governança e favorece ações mais seguras e transparentes no gerenciamento informacional.

Avançando nesse debate, Arruda et al. (2022) destacam que modelos robustos de segurança dependem da integração entre tecnologias, políticas internas e marcos regulatórios. A LGPD estabelece fundamentos obrigatórios para o tratamento de dados, enquanto o Bacen detalha parâmetros dirigidos ao setor bancário, promovendo alinhamento entre proteção informacional e conformidade regulatória. Essa

21

Salvador
2025

articulação incentiva a adoção de práticas que ampliam a prevenção de incidentes e fortalecem o amadurecimento institucional diante das novas exigências legais.
Em linha semelhante, Iurovschi, Nascimento e Carvalho (2022) argumentam que o desempenho financeiro das instituições está associado à qualidade da gestão de riscos, especialmente no que se refere ao tratamento de dados sensíveis. A LGPD introduz requisitos mais rígidos sobre uso e compartilhamento de informações, ao passo que o Bacen estabelece mecanismos de supervisão e monitoramento que ampliam a transparência das operações. Essa convergência normativa transforma a proteção de dados em componente estratégico para a estabilidade e a confiança depositada no sistema bancário.
A perspectiva de Pereira, Silva e Pinto (2025) reforça que a efetividade dos controles internos depende de políticas institucionais alinhadas às regulamentações aplicáveis ao setor financeiro. As resoluções do Bacen e do CMN, ao definirem padrões de governança e auditoria, fortalecem a atuação institucional ao tornar mais claro o conjunto de responsabilidades relacionadas ao tratamento de dados. Dessa forma, a conformidade com a LGPD ultrapassa a esfera jurídica e se consolida como prática de integridade, transparência e segurança informacional.
Em continuidade às análises sobre as implicações regulatórias, Souza et al. (2024) observam que a adequação à LGPD requer equilíbrio entre inovação tecnológica e responsabilidade institucional, sobretudo no ambiente bancário, no qual o tratamento de dados assume grande escala. As normas do Bacen orientam esse processo ao estabelecer parâmetros para segurança, gestão de riscos e práticas operacionais, criando condições para maior confiabilidade. Essa estrutura normativa, ao se alinhar aos princípios da LGPD, assegura que os sistemas de informação operem com transparência e integridade.
Beltrao (2025) enfatiza que a existência de um ambiente regulatório robusto depende da interação entre normas gerais e regras específicas aplicáveis ao sistema financeiro. O Bacen e o CMN, ao definirem diretrizes que disciplinam procedimentos técnicos e administrativos, permitem que a proteção de dados seja incorporada à rotina das instituições. Essa convergência assegura que a LGPD seja implementada de forma efetiva, promovendo estabilidade e fortalecendo a confiança dos titulares de

dados nas operações realizadas pelas entidades bancárias.

2.2 COMPLEXIDADE DOS SISTEMAS BANCÁRIOS E DESAFIOS DE INTEGRAÇÃO

A criação do BCBS 239 foi mais um marco importante em se tratando de segurança no mundo financeiro, pois trata-se de um framework (conjunto estruturado de diretrizes, princípios) internacional elaborado pelo Basel Committee on Banking Supervision (Comitê de Basileia), cujo objetivo é estabelecer princípios para o agregamento eficaz de dados de risco (risk data aggregation) e para a capacidade de reporte de informações (risk reporting) pelas instituições financeiras. Publicado em 2013, o documento surgiu após a crise financeira de 2008, quando se identificou que muitos bancos não possuíam sistemas integrados e confiáveis para consolidar informações de risco, dificultando a tomada de decisões e a supervisão prudencial.
O framework define 14 princípios que tratam de governança, qualidade e integridade de dados, infraestrutura tecnológica, precisão, completude, tempestividade, adaptabilidade e transparência das informações. Em síntese, o BCBS 239 busca assegurar que bancos de grande porte ou de relevância sistêmica tenham arquiteturas de dados integradas, processos padronizados e capacidade de gerar relatórios de risco consistentes, o que reduz vulnerabilidades e aumenta a solidez do sistema financeiro.
Mediante isso, a complexidade estrutural dos sistemas bancários decorre da coexistência de múltiplos bancos de dados históricos e plataformas tecnológicas heterogêneas, muitas delas desenvolvidas em contextos de baixa padronização. Beltrao (2025), ao analisar o framework BCBS239, observa que a fragmentação sistêmica prejudica a acurácia e a consistência das informações, afetando diretamente a capacidade de conformidade regulatória. Esse cenário é ainda mais agravado quando instituições lidam com dados provenientes de décadas de operação, acumulando redundâncias e inconsistências difíceis de tratar.
Os sistemas legados (sistemas de informação antigos), apesar de funcionais, representam entraves importantes à modernização, pois nem sempre dialogam
23

Salvador
2025

adequadamente com soluções mais recentes. Iurovschi, Nascimento, Carvalho (2022), ao examinarem bancos nepaleses, destacam que muitos ambientes financeiros ainda dependem de infraestruturas antigas, que não suportam demandas contemporâneas de rastreabilidade e auditoria. Essa dificuldade também se aplica ao setor bancário brasileiro, onde o legado tecnológico convive com iniciativas modernas, gerando lacunas de interoperabilidade.
A interoperabilidade entre plataformas internas constitui um dos principais desafios para garantir governança de dados sólida. Brandt e Vidotti (2024) argumentam que arquiteturas fragmentadas diminuem a confiabilidade das informações utilizadas para fins regulatórios, especialmente quando não há

mecanismos robustos de integração orientados por modelos de linhagem de dados. Essa ausência compromete análises de risco, auditorias e a própria implementação dos princípios da LGPD.

A integração entre plataformas externas também se revela complexa, sobretudo em ambientes multicloud. Silva et al., (2025) demonstra que arquiteturas distribuídas exigem mecanismos automatizados de rastreamento de dados, pois o fluxo informacional se desloca continuamente entre diferentes provedores de nuvem. No setor bancário, esse dinamismo se intensifica devido ao uso simultâneo de soluções internas, APIs de parceiros (interfaces utilizadas para permitir a comunicação padronizada entre sistemas distintos), fintechs (bancos digitais) e sistemas regulatórios.

No ambiente regulado pelo Bacen ? especialmente após o Open Finance ? as fintechs se tornam atores essenciais na cadeia de valor, pois desenvolvem serviços que dependem de APIs bancárias, compartilhamento de dados e arquiteturas distribuídas, intensificando a necessidade de padronização e governança de dados. No mais, o rastreamento do fluxo completo dos dados é outro ponto sensível. A ausência de visibilidade integral impede que instituições compreendam com precisão onde e como os dados trafegam, o que compromete análises de impacto e medidas de mitigação. Segundo Brandt e Vidotti (2024), a falta de sistemas de data lineage (rastreabilidade de dados) por se tratar de sistemas que trazem soluções tecnológicas que permitem mapear, registrar e visualizar todo o caminho percorrido

24

Salvador
2025

por um dado dentro de uma organização dificulta a identificação de responsáveis por modificações, transformações e compartilhamentos indevidos.

Alves et al. (2022), ao analisarem aplicações da tecnologia blockchain (tecnologia de registro distribuído que armazena dados em blocos encadeados de forma imutável e segura, sem controle central) na área da saúde, evidenciam que a fragmentação dos sistemas informacionais compromete a confiabilidade dos registros e reduz a eficiência dos processos decisórios. Embora o estudo esteja voltado ao setor da saúde, o argumento sobre a importância de dados integrados, auditáveis e estruturados é plenamente aplicável ao contexto bancário, no qual a precisão e a rastreabilidade das informações são fundamentais para operações de crédito, segurança cibernética e prevenção a fraudes.

A expansão do open finance (modelo de compartilhamento padronizado de dados e serviços financeiros entre instituições, mediante consentimento do usuário) acrescenta outra camada de complexidade. Como dados passam a circular entre instituições distintas, a integração precisa assegurar padrões consistentes de

segurança, governança e rastreamento. As reflexões de Beltrao (2025) sobre padronização e governança reforçam que ambientes informacionais abertos exigem regras claras e mecanismos automáticos para evitar incompatibilidades e riscos sistêmicos.
Assim, a complexidade dos sistemas bancários não reside apenas na multiplicidade de tecnologias, mas também na ausência de infraestrutura adequada para rastreamento e interoperabilidade. As contribuições de Silva et al., (2025) e Brandt e Vidotti (2024) revelam que a modernização tecnológica exige não apenas ferramentas novas, mas também revisões profundas na arquitetura de dados. Dessa forma, os desafios estruturais convertem-se em obstáculos diretos ao cumprimento da LGPD.

2.2.1 Riscos cibernéticos e incidentes de segurança

O ambiente bancário figura entre os mais suscetíveis a ataques cibernéticos, dado o valor econômico dos dados e a constante tentativa de violação por agentes

maliciosos. Carmo (2021), ao analisarem sistemas críticos, demonstram que vulnerabilidades estruturais podem ser exploradas por meio de ataques sofisticados de ransomware (tipo de malware que sequestra dados, criptografa arquivos e exige pagamento para liberar o acesso) e phishing (técnica fraudulenta que visa enganar o usuário para obter dados sensíveis, geralmente por meio de mensagens ou links falso). Em bancos, esses riscos são ampliados pela dependência crescente de interfaces digitais, como aplicativos e plataformas de internet banking.
Ataques de engenharia social permanecem especialmente eficazes, pois exploram fragilidades humanas e lacunas nos processos internos de autenticação. Iurovschi, Nascimento, Carvalho (2022), ao estudarem bancos nepaleses, destacaram que falhas operacionais e comportamentais contribuem significativamente para incidentes de segurança, muitas vezes tanto quanto vulnerabilidades tecnológicas. Esse paralelo se aplica ao contexto brasileiro, onde a diversidade de perfis de usuários amplia o vetor de ataque.
As APIs, essenciais para integração em open finance, também constituem pontos frágeis quando não apropriamente protegidas. Brandt e Vidotti (2024) argumentam que fluxos externos mal monitorados podem gerar brechas de segurança, permitindo acesso indevido a informações sensíveis. Em setores altamente regulados, como o bancário, essa exposição pode comprometer a integridade das operações.

Em aplicativos mobile, a diversidade de dispositivos e sistemas operacionais cria um ambiente heterogêneo que dificulta a padronização de medidas de segurança. Silva et al., (2025) enfatiza que ambientes multicloud já apresentam desafios de consistência; quando combinados a aplicações móveis, o risco se multiplica. A ampliação de funcionalidades nos aplicativos tende a aumentar a superfície de ataque.
O monitoramento contínuo é apontado por Carmo (2021) como elemento indispensável para mitigar riscos em sistemas críticos. Ferramentas automatizadas de detecção, associadas a testes permanentes de vulnerabilidade, permitem identificar comportamentos anômalos e corrigir falhas antes que sejam exploradas em grande escala. No setor bancário, a natureza contínua das transações torna esse
26

Salvador
2025

monitoramento ainda mais essencial.
Alves et al. (2022) destacam que sistemas auditáveis e distribuídos fortalecem a resiliência, pois reduzem riscos de perda ou manipulação indevida de dados. Embora estudem blockchain no contexto da saúde, o princípio de segurança descentralizada pode ser aplicado aos bancos como estratégia complementar de proteção. A descentralização tende a dificultar ataques coordenados que dependem de alvos únicos.
Beltrao (2025) complementa que a segurança não depende apenas de medidas técnicas, mas de uma estrutura de governança capaz de detectar e responder rapidamente a incidentes. Para o setor bancário, isso significa articular equipes especializadas, planos de resposta a incidentes e comunicação transparente com órgãos reguladores. A velocidade de resposta pode determinar a extensão dos danos.
Em síntese, os riscos cibernéticos enfrentados pelos bancos revelam uma combinação de fatores técnicos, comportamentais e organizacionais. A integração das perspectivas de Carmo, Alves, Beltrao, Nascimento e D?alkmin Neves mostra que a segurança eficiente depende da convergência entre tecnologia avançada, avaliação contínua e cultura institucional. Assim, a LGPD amplia a necessidade de vigilância permanente, reforçando que segurança e governança devem operar de forma indissociável.

2.2.2 Barreiras jurídico-regulatórias e compliance interno

A conformidade regulatória no setor bancário demanda harmonização entre múltiplas normas, o que representa desafio contínuo para as instituições. O diálogo entre LGPD, Banco Central e Código de Defesa do Consumidor não é simples, pois

cada norma opera com enfoques distintos. Beltrao (2025) aponta que, mesmo em padrões internacionais, a consolidação de regras de conformidade exige estruturação robusta e alinhamento sistêmico, algo que no Brasil assume contornos ainda mais complexos.

O Código de Defesa do Consumidor estabelece princípios de máxima proteção. Entre eles destacam-se os princípios da transparência e da informação, que obrigam

27

Salvador
2025

os fornecedores a disponibilizarem dados claros, completos e compreensíveis sobre a utilização de informações pessoais e sobre os riscos inerentes aos serviços prestados. Soma-se a isso o princípio da boa-fé objetiva, que exige condutas leais e previsíveis no tratamento de dados, e o princípio da segurança, que determina a adoção de mecanismos eficazes de proteção contra falhas sistêmicas, vazamentos e ataques cibernéticos.

Por fim, o CDC incorpora a responsabilidade objetiva dos fornecedores, tornando as instituições bancárias responsáveis por danos decorrentes de falhas no serviço, independentemente de culpa. Enquanto a LGPD introduz novos critérios de transparência e finalidade, como a exigência de objetivos específicos para cada tratamento, a ampliação das obrigações informacionais ao titular, a minimização de dados, a necessidade de comprovação contínua de conformidade (accountability) e a adoção de medidas robustas de segurança e rastreabilidade, Brandt e Vidotti (2024) explicam que a ausência de padrões claros de linhagem de dados dificulta a comprovação de cumprimento das normas, especialmente em incidentes que envolvem múltiplos fluxos informacionais. Essa falta de visibilidade cria vulnerabilidades jurídicas e operacionais.

As normas do Banco Central, por sua vez, impõem requisitos técnicos que demandam investimentos contínuos. Iurovschi, Nascimento, Carvalho (2022) demonstram que instituições financeiras já enfrentam pressões para manter indicadores estáveis em cenários de estresse. Acrescentar a isso exigências estruturais de segurança e rastreabilidade implica redefinição de prioridades orçamentárias.

Alves et al. (2022) mostram que, mesmo em setores distintos, a adoção de tecnologias sofisticadas gera custos elevados, principalmente em transições que envolvem infraestrutura antiga. No setor bancário, essa realidade é evidente: modernizar sistemas, integrar plataformas e implementar governança exige investimentos constantes. O custo não é apenas financeiro, mas também organizacional e temporal.

Silva et al., (2025) observa que ambientes multicloud ampliam a complexidade

jurídica, pois envolvem provedores externos, contratos híbridos e regras diferentes de
28

Salvador
2025

responsabilidade. Essa multiplicidade de territórios jurídicos dificulta a aplicação homogênea da LGPD e inviabiliza modelos simples de atribuição de responsabilidades. A depender do fluxo dos dados, a cadeia de custódia pode se tornar difícil de demonstrar.
Outro desafio é a ressiginificação de práticas automatizadas, como perfis comportamentais utilizados em crédito. Brandt e Vidotti (2024) afirmam que a opacidade dos modelos de IA compromete a transparência exigida pela LGPD. No ambiente bancário, decisões automatizadas impactam diretamente concessão, limite e risco, o que gera exigência regulatória dupla: precisão técnica e justificativa jurídica. Iurovschi, Nascimento, Carvalho (2022) destacam que a volatilidade dos mercados pressiona bancos a adotarem soluções rápidas, o que nem sempre se concilia com os procedimentos exigidos pelas normas de proteção de dados. Essa tensão entre urgência operacional e conformidade regulatória evidencia que o compliance precisa ser dinâmico e adaptativo, e não apenas burocrático.
Assim, as barreiras jurídico-regulatórias enfrentadas pelos bancos resultam de uma convergência entre normas diversas, alta complexidade estrutural e necessidade de atualização permanente. A análise conjunta dos autores demonstra que compliance, no setor financeiro, não se resume a cumprir regras, mas requer governança contínua, documentação robusta e adaptação constante. A LGPD, nesse cenário, reforça a necessidade de estruturas mais maduras e transparentes.

2.3 FORTALECIMENTO DA INFRAESTRUTURA TECNOLÓGICA DE PROTEÇÃO DE DADOS

As estratégias de fortalecimento da infraestrutura tecnológica nas instituições bancárias vêm sendo crescentemente orientadas por arquiteturas de segurança mais rígidas, capazes de responder a um cenário de ameaças sofisticadas e contínuas. Souza et al. (2024) destacam que a LGPD acelera a adoção de soluções tecnológicas avançadas, pois a responsabilização jurídica passa a estar diretamente vinculada à capacidade técnica de proteção. Desse modo, criptografia robusta, tokenização e armazenamentos seguros deixam de ser diferenciais competitivos para se tornar componentes estruturais da governança de dados.
29

Salvador

2025

A arquitetura Zero Trust surge, nesse contexto, como paradigma relevante para o setor financeiro. Segundo Arruda et al., (2022), o modelo rompe com a lógica de confiança implícita em redes internas, adotando a premissa de que nenhum dispositivo, usuário ou aplicação deve ser considerado confiável por padrão. Nascimento e D?alkmin neves (2025) complementam que, em ambientes distribuídos e híbridos, essa abordagem reduz consideravelmente vetores de ataque, pois cada acesso é continuamente autenticado, autorizado e monitorado. Para bancos, essa lógica é particularmente útil diante da multiplicidade de canais digitais e integrações externas.

A implementação de Zero Trust, contudo, enfrenta desafios técnicos e organizacionais. Nascimento e D?alkmin neves (2025) apontam que a transição exige mapeamento detalhado de ativos, redefinição de políticas de acesso e reestruturação de redes legadas. No setor bancário, essa complexidade é ampliada por sistemas antigos, integrações com parceiros e requisitos de alta disponibilidade. Nesse sentido, a adoção do modelo não pode ser vista como mera substituição tecnológica, mas como processo gradual de reconfiguração da arquitetura de segurança.

A proteção multicamadas também se impõe como princípio estruturante. Arruda et al., (2022) enfatizam que a combinação de mecanismos de perímetro, segmentação de rede, autenticação forte e monitoramento contínuo proporciona defesas redundantes, capazes de mitigar falhas pontuais. Em instituições financeiras, onde incidentes podem produzir impactos sistêmicos, essa redundância torna-se elemento essencial de resiliência. A ideia de ?defesa em profundidade? converge, assim, com as exigências regulatórias de proteção de dados pessoais.

Criptografia e tokenização constituem, ainda, ferramentas centrais para reduzir o impacto de eventuais acessos indevidos. Souza et al. (2024) assinalam que a LGPD não exige apenas a prevenção de incidentes, mas também medidas que minimizem danos quando eles ocorrem. Ao embaralhar dados em trânsito e em repouso, e ao substituir identificadores sensíveis por tokens, as instituições bancárias conseguem reduzir a exposição real de informações mesmo em cenários de violação.

A adoção de soluções de detecção e resposta a incidentes, como EDR (ferramenta de monitoramento contínuo que detecta, investiga e responde a ameaças

30

Salvador
2025

em endpoints, como computadores e servidores) e SIEM (sistema que coleta e correlaciona logs de diferentes fontes para identificar incidentes de segurança e gerar alertas em tempo real), complementa essa infraestrutura. Nascimento e D?alkmin

neves (2025) indicam que, em arquiteturas Zero Trust, a visibilidade contínua é tão importante quanto o bloqueio preventivo. Ferramentas de correlação de eventos e análise em tempo real permitem identificar padrões anômalos, acelerar respostas e produzir trilhas de auditoria relevantes para fins regulatórios. Em bancos, esse monitoramento é fundamental para conciliar velocidade transacional com segurança. Souza et al. (2024) ressaltam que a integração entre tecnologias de segurança e requisitos da LGPD demanda alinhamento entre áreas jurídicas, de TI e de negócios. Não basta implementar ferramentas sofisticadas; é necessário que elas estejam articuladas com políticas internas de retenção, minimização e finalidade. Assim, a infraestrutura tecnológica passa a ser um braço operacional da governança, e não um conjunto isolado de soluções técnicas.
Por fim, as contribuições de Arruda et al., (2022) e Nascimento e D?alkmin neves (2025) convergem ao mostrar que o fortalecimento da infraestrutura tecnológica não é um evento pontual, mas um processo contínuo de adaptação. No setor bancário, isso implica revisitar periodicamente configurações, políticas de acesso e modelos de ameaça, em diálogo com as exigências da LGPD e com a evolução das práticas de cibersegurança. A infraestrutura tecnológica, nesse sentido, torna-se eixo dinâmico da governança de dados.

2.3.1 Implementação de políticas internas e cultura de privacidade

A consolidação de políticas internas consistentes é condição indispensável para que as soluções tecnológicas realmente resultem em proteção efetiva de dados. Rampini et al. (2024) destacam que programas de compliance estruturados, alinhados a normas como a ISO 37301:2021, ampliam a capacidade de coordenação entre processos, pessoas e tecnologias. No contexto bancário, essa articulação é crucial para garantir que a LGPD não seja apenas um texto normativo, mas um conjunto de práticas incorporadas ao cotidiano organizacional.
31

Salvador
2025

A cultura de privacidade depende, em grande medida, de processos formativos contínuos. Souza et al. (2024) enfatizam que a LGPD insere a dimensão tecnológica no centro do debate jurídico, exigindo que profissionais de diferentes áreas compreendam minimamente os riscos associados ao tratamento de dados. Assim, treinamentos periódicos, reciclagens e campanhas internas tornam-se instrumentos para reduzir falhas humanas, que seguem sendo relevantes vetores de incidentes. Freitas e Filho (2018) chamam atenção para o papel da auditoria interna na avaliação da ?risk culture? no setor financeiro. Mais do que verificar aderência formal

a normas, a auditoria deve observar comportamentos, atitudes e decisões cotidianas que revelam como o risco é percebido e gerido. Essa perspectiva é essencial para entender se políticas de privacidade e segurança realmente informam práticas, ou se permanecem apenas como documentos formais.
Comitês de segurança e governança de dados emergem como estruturas importantes para coordenar ações e decisões estratégicas. Sousa et al. (2024), ao analisar a evolução da divulgação de práticas de compliance em companhias brasileiras, mostram que a institucionalização de instâncias colegiadas contribui para maior transparência e coerência nas políticas. Em instituições bancárias, com múltiplas áreas de negócio, esses comitês ajudam a alinhar diretrizes de privacidade a objetivos corporativos mais amplos.
Pereira et al., (2025) evidenciam que sistemas de auditoria interna robustos contribuem diretamente para o fortalecimento da governança corporativa. A partir de seu estudo em instituições educacionais, os autores demonstram que a auditoria atua como mecanismo de monitoramento contínuo e de correção de desvios. Transposta para o ambiente bancário, essa lógica indica que auditorias focadas em proteção de dados podem identificar fragilidades antes que se convertam em violações graves.
A padronização de rotinas de auditoria, risco e compliance é outro aspecto enfatizado por Rampini et al. (2024). A ausência de critérios uniformes dificulta comparações, relatórios e análises históricas, comprometendo a capacidade de aprendizagem institucional. Programas de integridade mais maduros estabelecem métricas, indicadores e ciclos regulares de avaliação, o que favorece a incorporação progressiva da privacidade como valor organizacional.
32

Salvador
2025

Sousa et al. (2024) apontam ainda que a pressão social e regulatória, intensificada no contexto pós-?Lava Jato?, levou empresas a tornarem mais visíveis suas práticas de compliance. Nos bancos, essa visibilidade pode se manifestar em relatórios de sustentabilidade, códigos de conduta, políticas de privacidade publicadas e canais de denúncia. Tais instrumentos reforçam a percepção de que o tema não é periférico, mas central para a imagem e a legitimidade institucional.
Assim, a implementação de políticas internas e o desenvolvimento de uma cultura de privacidade dependem da convergência entre formação, auditoria, comitês de governança e padronização de processos. As contribuições de Rampini et al. (2024), Freitas e Filho (2018), Sousa et al. (2024) e Pereira et al., (2025) convergem na ideia de que a governança de dados é tanto uma questão de estruturas formais quanto de valores e práticas internalizados. No setor bancário, esse alinhamento é determinante para a efetividade da LGPD.

2.3.2 Modernização do relacionamento com o titular e transparência

A modernização do relacionamento com o titular de dados exige que transparência e controle deixem de ser apenas obrigações legais para se converterem em diferenciais de confiança. Souza et al. (2024) sustentam que a LGPD reposiciona o titular como sujeito de direitos em ambientes altamente tecnologizados, exigindo canais claros de informação e participação. No setor bancário, essa mudança repercute diretamente sobre contratos, interfaces digitais e rotinas de atendimento. Notificações claras sobre coleta e uso de dados tornam-se centrais nesse processo. Matos (2022), ao discutir avaliação automatizada da conformidade de aplicativos móveis com requisitos de privacidade, mostra que avisos genéricos e pouco compreensíveis tendem a ser ineficazes para proteger o usuário. Em aplicativos bancários, onde decisões financeiras são tomadas a partir de dados pessoais, a clareza comunicativa assume peso ainda maior.
Ferramentas digitais de controle, consentimento e portabilidade também compõem esse novo cenário. Souza et al. (2024) destacam que a tecnologia, antes vista apenas como vetor de risco, passa a ser igualmente meio de ampliar o poder de
33

Salvador
2025

decisão do titular. Painéis de controle, dashboards de privacidade e opções configuráveis de compartilhamento de dados permitem que o cliente visualize e gerencie, em tempo quase real, o uso de suas informações.
Matos (2022) argumenta que a automação da verificação de requisitos de privacidade em aplicativos é caminho promissor para garantir conformidade de forma sistemática. Transpondo essa lógica para o contexto bancário, é possível imaginar mecanismos que avaliem continuamente se interfaces e fluxos de dados atendem às exigências de transparência e consentimento da LGPD. Isso reduziria dependência exclusiva de revisões manuais, sujeitas a falhas e desatualizações.
A comunicação proativa após incidentes também é elemento chave da transparência. Sousa et al. (2024) mostram que, em contextos de forte escrutínio público, organizações passaram a adotar postura mais aberta na divulgação de práticas de compliance. No caso de vazamentos de dados bancários, informar rapidamente o ocorrido, seus impactos e as medidas adotadas contribui para preservar, ao menos parcialmente, a confiança do cliente e dos reguladores. Relatórios de segurança e de governança de dados podem funcionar como extensões dessa comunicação, oferecendo uma visão mais ampla das ações empreendidas pelas instituições. Rampini et al. (2024) indicam que relatórios

estruturados, alinhados a padrões internacionais de compliance, permitem que stakeholders avaliem o grau de maturidade dos programas de integridade. Aplicados ao setor bancário, esses instrumentos reforçam a ideia de prestação de contas contínua.

Souza et al. (2024) também enfatizam que a modernização do relacionamento com o titular passa por reconhecer a assimetria informacional existente entre instituições e clientes. Por isso, a simples disponibilização de políticas complexas não é suficiente; é necessário investir em linguagem acessível, recursos visuais e suportes educativos. Essa preocupação aproxima o discurso jurídico do cotidiano das pessoas, tornando a proteção de dados um tema mais inteligível.

Dessa forma, as estratégias de modernização do relacionamento com o titular e de promoção da transparência articulam tecnologia, comunicação e governança. A partir das contribuições de Matos (2022), Souza et al. (2024), Sousa et al. (2024) e

34

Salvador
2025

Rampini et al. (2024), percebe-se que bancos que investem em canais claros, ferramentas de controle e comunicação proativa não apenas atendem à LGPD, mas também fortalecem laços de confiança em um ambiente financeiro cada vez mais digitalizado.

35

Salvador
2025

3 CONCLUSÃO

A análise desenvolvida ao longo deste estudo permitiu concluir que a pergunta-problema foi plenamente respondida, demonstrando que os desafios enfrentados pelas instituições bancárias na aplicação da LGPD decorrem de fatores interligados: complexidade sistêmica, riscos cibernéticos persistentes e barreiras jurídico-regulatórias que demandam governança integrada. Os objetivos específicos também foram contemplados, uma vez que se identificaram as exigências legais mais relevantes para o setor, examinaram-se as dificuldades operacionais e tecnológicas que afetam a conformidade e analisaram-se as principais estratégias adotadas pelos bancos para fortalecer sua segurança e governança de dados. As discussões evidenciaram que a implementação efetiva da LGPD no ambiente financeiro depende tanto da modernização contínua das infraestruturas tecnológicas quanto da

consolidação de uma cultura institucional voltada à privacidade, à transparência e à responsabilização.
Nesse sentido, observou-se que as instituições bancárias avançaram na adoção de soluções como arquiteturas Zero Trust, mecanismos de criptografia, sistemas de monitoramento e políticas internas de compliance, mas ainda enfrentam desafios significativos relacionados à integração de sistemas legados, à mitigação de riscos cibernéticos e à padronização de práticas de governança. A modernização do relacionamento com o titular, com ênfase em transparência e comunicação proativa, mostrou-se essencial para fortalecer a confiança e reduzir assimetrias informacionais, mas ainda carece de aprimoramentos estruturais e comunicacionais.
Considerando essas constatações, sugerem-se trabalhos futuros voltados à investigação da maturidade da governança de dados em instituições de diferentes portes, bem como estudos comparativos entre bancos tradicionais e fintechs sobre práticas de segurança e privacidade. Pesquisas empíricas envolvendo a percepção dos titulares sobre transparência, consentimento e confiança também podem enriquecer a compreensão do impacto real da LGPD no setor financeiro. Ademais, análises aprofundadas sobre a relação entre inteligência artificial, decisões automatizadas e proteção de dados emergem como campo promissor, especialmente
36

Salvador
2025

diante do crescimento de modelos preditivos no crédito bancário. Assim, abre-se espaço para que novos estudos consolidem o entendimento sobre os caminhos que o setor deve trilhar para alcançar conformidade plena e governança mais robusta.

37

Salvador
2025

REFERENCIAS BIBLIOGRAFICAS

ALMEIDA, R.; MOTTA, A. LGPD e compliance empresarial: os desafios de adequação à nova dinâmica de proteção de dados e as atuais perspectivas de responsabilização empresarial. 2022. DOI: 10.29327/iicoloquiobrasilfrancaeiimostra.455416.
ALVES, Charles Jefferson Rodrigues; PINTO DOS REIS, Leandro Teófilo; NETO, Levi Rodrigues; DA SILVA, Débora Oliveira; DA COSTA, Cristiano André. Blockchain em saúde: uma análise de pesquisas na base Scopus. Journal of Health

Informatics, Brasil, v. 14, n. 2, 2022. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/935. Acesso em: 26 nov. 2025.
ARRUDA, Luiz Guilherme Schiefler de; GIOZZA, William Ferreira; AMVAME NZE, Georges Daniel; NUNES, Rafael Rabelo. Implementação da Arquitetura Zero Trust: uma revisão sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf. Acesso em: 26 nov. 2025.
BELTRAO, Raquel Cesario. O controle e consentimento: os desafios da implantação da LGPD nas instituições financeiras no Brasil e sua gestão de riscos. Revista Ibmec de Direito, v. 1, n. 2, 2025. Disponível em: https://ibmec.periodicoscientificos.com.br/index.php/cienciajuridica/article/view/240. Acesso em: 26 nov. 2025.
BRANDT, M. B.; VIDOTTI, S. A. B. G. Arquitetura da informação para processos de negócio e modelagem de banco de dados: aproximações possíveis. Em Questão, v. 30, e131304, 2024. Disponível em: https://doi.org/10.1590/1808-5245.30.131304. Acesso em: 26 nov. 2025.
CARMO, Ubiratan Alves; SIQUEIRA, Iony Patriota; MARINHO, Manoel Henrique Nóbrega; RISSI, Guilherme Ferretti; TOMASIN, Samuel Giuseppe. Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI. Revista Brasileira de Engenharia ? Engenharias IV: Engenharia Elétrica, Sistemas Elétricos de Potência e Eletrônica de Potência, n. 55, 2021. Disponível em: https://doi.org/10.18265/1517-0306a2021id4764. Acesso em: 26 nov. 2025.
DEPRÁ, C. O encarregado pelo tratamento de dados pessoais na administração pública: um agente de efetivação da governança no tratamento de dados pessoais dos administrados. Revista Caderno Pedagógico, v. 22, n. 11, 2025. DOI: 10.54033/cadpedv22n11-050.
FARIAS, L.; OLIVEIRA, G. Como o design da informação pode contribuir no entendimento dos titulares de dados na LGPD. 2024. DOI: 10.5151/cidiconcic2023-107_645653.
38

Salvador
2025

FREITAS, C.; MAFFINI, M. A proteção dos dados pessoais no crédito bancário e a LGPD frente ao cadastro positivo. Revista Jurídica Cesumar, v. 20, n. 1, p. 29-42, 2020. DOI: 10.17765/2176-9184.2020v20n1p29-42.
FREITAS, Volnei Adriano de; FONTES FILHO, Joaquim Rubens. A função de auditoria interna na governança corporativa de bancos no Brasil: agente de controle ou instrumento de legitimidade organizacional? Cadernos Gestão Pública e

Cidadania, v. 29, n. 3, 2018. Disponível em: https://doi.org/10.22561/cvr.v29i3.4245. Acesso em: 26 nov. 2025.
IUROVSCHI, Yuri Zanolini; NASCIMENTO, Rafael Pagliarini do; CARVALHO, Flávio Leonel de. Desempenho financeiro de bancos brasileiros em períodos de crise: avaliação a partir dos indicadores CAMEL. CONTABILOMETRIA ? Brazilian Journal of Quantitative Methods Applied to Accounting, Monte Carmelo, v. 9, n. 2, p. 63-83, jul./dez. 2022. Disponível em: https://revistas.fucamp.edu.br/index.php/contabilometria/article/view/2620/1679. Acesso em: 26 nov. 2025.
MATOS, Eurico. Aplicativos móveis governamentais e a proteção de dados pessoais: entre políticas de privacidade, trackers e permissões. 2022. Disponível em: https://www.researchgate.net/publication/358411971_Aplicativos_moveis_governamentais_e_a_protecao_de_dados_pessoais_Entre_politicas_de_privacidade_trackers_e_permissoes. Acesso em: 26 nov. 2025.
MENDES, A.; JÚNIOR, V. LGPD: uma análise crítica da sua implementação e efetividade no combate ao vazamento de dados. 2024. DOI: 10.62140/amvj442024.
NASCIMENTO, E.; D?ALKMIN NEVES, J. E. Arquitetura Zero Trust: boas práticas de gestão de riscos de segurança da informação. Revista Brasileira em Tecnologia da Informação, v. 6, n. 1, p. 69-82, 2025. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/127. Acesso em: 26 nov. 2025.
PEREIRA, E. J. D.; SILVA, R. C. L.; PINTO, D. S. A. Auditoria interna e sistemas de controle: caminhos para o fortalecimento da transparência corporativa. Revista Foco, v. 18, n. 10, p. e10323, 2025. DOI: 10.54751/revistafoco.v18n10-200. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/10323. Acesso em: 26 nov. 2025.
PILO?, F. Segurança da informação no setor público e adequação à LGPD. Revft, v. 29, n. 146, p. 30-31, 2025. DOI: 10.69849/revistaft/dt10202505272130.
RAMPINI, G. et al. Análise bibliométrica sobre o papel da gestão de riscos nos programas de compliance com o advento da ISO 37301:2021. Brazilian Applied Science Review, v. 8, n. 1, p. 130?147, 2024. DOI: 10.34115/basrv8n1-007.
SILVA, D.; FALCÃO, E. Análise construtiva da Lei Geral de Proteção de Dados.
39

Salvador
2025

Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 10, p. 5042-5064, 2024. DOI: 10.51891/rease.v10i10.16270.
SILVA, Hudson A. B. da; JOCHEM, José E. M.; SANTOS, João V. dos; SOUSA,

Eduardo F. R. de; MELLO, Ronaldo dos S.; DORNELES, Carina F.; FILETO, Renato. Uma abordagem para a gestão da linhagem de dados heterogêneos. In: BRAZILIAN SYMPOSIUM ON DATA BASES ? SBBD, 40., 2025, Fortaleza. Proceedings of the 40th Brazilian Symposium on Data Bases. Fortaleza, 2025. DOI: https://doi.org/10.5753/sbbd.2025.247293.

SOUSA, H. et al. A evolução na divulgação de práticas de compliance por companhias abertas brasileiras no período ?Lava Jato?. Cadernos EBAPE.BR, v. 22, n. 1, 2024. DOI: 10.1590/1679-395120230041.

SOUZA, A. et al. O futuro do direito: novas tecnologias e a Lei Geral de Proteção de Dados. Delos ? Desarrollo Local Sostenible, v. 17, n. 58, e1622, 2024. DOI: 10.55905/rdelosv17.n58-009.

TEIXEIRA, L. et al. Proposta de um repositório digital para transparência de dados pessoais. 2023. DOI: 10.5753/wide.2023.236108.