PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

LEI GERAL DE PROTEÇÃO DE DADOS E A SEGURANÇA DA INFORMAÇÃO: ATUAÇÃO DO GESTOR DE TECNOLOGIA DA INFORMAÇÃO

GENERAL DATA PROTECTION LAW AND INFORMATION SECURITY: PERFORMANCE OF THE INFORMATION TECHNOLOGY MANAGER

Marcos Gabriel Chieratto Cavenaghi[1], Lucio Rogerio Pelizer Paris[2], Wladimir José Camillo Menegassi[3], Joaquim M. F. Antunes Neto[4], Luiz Henrique Biazotto[5]

1- Formando do CST em Gestão da Tecnologia da Informação da FATEC Itapira; 2- Especialista em Engenharia de Sistemas, ESAB, Brasil. Docente da ETEC Itapira e FATEC Itapira; 3- Mestre no Programa de Mestrado Multiprofissional em Saúde e Educação, UNAERP, Ribeirão Preto, São Paulo. Especialista em Gestão Empresarial. Docente da FATEC Itapira; 4- Doutor em Biologia Funcional e Molecular, IB, UNICAMP, Campinas, São Paulo. MBA em Gestão de Estratégia Empresarial e Especialista em Tecnologias para a Indústria 4.0. Docente e orientador na FATEC Itapira; 5- Mestrado Profissional em Gestão de Redes de Teleco, Pontifícia Universidade Católica de Campinas, Campinas, São Paulo. Diretor da FATEC Itapira, docente e orientador.

Contato: joaquim.antunes@fatec.sp.gov.br

RESUMO

Este trabalho tem como objetivo analisar o impacto da Lei Geral de Proteção de Dados (LGPD) na segurança da informação e o papel do gestor de tecnologia da informação (TI) na conformidade com esta legislação. A LGPD, em vigor desde setembro de 2020, estabelece regras e diretrizes para o tratamento de dados pessoais, visando proteger a privacidade e os direitos dos indivíduos. Com o aumento das ameaças cibernéticas e a crescente quantidade de dados gerados e compartilhados, torna-se fundamental para as organizações garantir a segurança e a integridade das informações. Nesse contexto, o gestor de TI desempenha um papel crucial, sendo responsável por implementar medidas de segurança da informação, garantir a conformidade com a LGPD e mitigar os riscos de violação de dados. Este estudo analisará as práticas e desafios enfrentados pelo gestor de TI na adequação às exigências da LGPD, explorando estratégias e melhores práticas para garantir a proteção dos dados e o cumprimento das normas legais. Ao final, espera-se contribuir para uma compreensão mais ampla do papel do gestor de TI na era da LGPD e para o desenvolvimento de estratégias eficazes de segurança da informação nas organizações.

Palavras-chave: Lei Geral de Proteção de Dados. Segurança da Informação. Gerenciamento de Riscos. Políticas de Segurança. Impacto Organizacional.

ABSTRACT

This work aims to analyze the impact of the General Data Protection Law (LGPD) on information security and the role of the information technology (IT) manager in compliance with this legislation. The LGPD, in force since September 2020, establishes rules and guidelines for the processing of personal data, aiming to protect the privacy and rights of individuals. With the rise of cyber threats and the increasing amount of data generated and shared, it becomes critical for organizations to ensure the security and integrity of information. In this context, the IT manager plays a crucial role, being responsible for implementing information security measures, ensuring

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

compliance with the LGPD, and mitigating the risks of data breaches. This study will analyze the practices and challenges faced by the IT manager in adapting to the requirements of the LGPD, exploring strategies and best practices to ensure data protection and compliance with legal standards. In the end, it is expected to contribute to a broader understanding of the role of the IT manager in the LGPD era and to the development of effective information security strategies in organizations.

Keywords: General Data Protection Law. Information Security. Risk Management. Security Policies. Organizational Impact.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil em agosto de 2018, representa um marco significativo na regulação do uso, armazenamento e compartilhamento de dados pessoais no país. Inspirada na legislação europeia (UNIÃO EUROPEIA, 2016), a *General Data Protection Regulation* (GDPR), a LGPD tem como objetivo principal garantir a privacidade e a proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo diretrizes claras sobre os direitos dos titulares de dados e as obrigações das organizações que os processam. A lei abrange todos os setores da economia, impactando empresas públicas e privadas que lidam com dados pessoais, independentemente do porte ou segmento de atuação (BRASIL, 2018).

A LGPD introduz uma série de princípios e bases legais para o tratamento de dados pessoais, exigindo que as organizações obtenham consentimento explícito dos titulares ou que demonstrem a necessidade do processamento de dados para finalidades específicas e legítimas, como a execução de contratos ou o cumprimento de obrigações legais. Além disso, a lei estabelece direitos aos titulares, como o acesso, correção e exclusão de seus dados, bem como a possibilidade de portabilidade e oposição ao tratamento de dados em determinadas circunstâncias. Para garantir a conformidade com a LGPD, as organizações devem adotar medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos, alterações e outros incidentes de segurança (ABNT, 2021).

A implementação da LGPD também criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por zelar pela aplicação da lei, promover a conscientização sobre a proteção de dados e fiscalizar as práticas das organizações. A ANPD tem o poder de aplicar sanções administrativas em caso de descumprimento da LGPD, que podem incluir advertências, multas significativas e a publicização da infração. Dessa forma, a LGPD não só fortalece os direitos dos titulares de dados, mas também impulsiona as organizações a adotarem uma postura mais ética e transparente no tratamento de dados pessoais, promovendo a confiança dos consumidores e a segurança jurídica no ambiente digital brasileiro (BRASIL, 2019).

No contexto da segurança da informação, a LGPD impõe exigências rigorosas às organizações para a implementação de medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas, alterações ou qualquer forma de tratamento inadequado ou ilícito. A lei enfatiza a importância de uma gestão de risco robusta e de uma cultura organizacional voltada para a privacidade e proteção de dados. Silva (2022) enfatiza

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

que entre as práticas recomendadas estão a adoção de políticas de segurança da informação, a realização de auditorias regulares, a capacitação contínua dos colaboradores e a utilização de tecnologias de segurança, como criptografia e controle de acesso.

Os profissionais de tecnologia da informação (TI) desempenham um papel fundamental na conformidade com a LGPD e na proteção dos dados pessoais. Eles são responsáveis por projetar e implementar sistemas e processos que garantam a segurança dos dados em todas as etapas de seu ciclo de vida. Além disso, os profissionais de TI devem colaborar estreitamente com outras áreas da organização, como jurídico e *compliance*, para assegurar que as políticas e procedimentos estejam alinhados com as exigências legais e regulatórias. A conscientização e o treinamento contínuo dos colaboradores sobre a importância da proteção de dados e as melhores práticas de segurança também são essenciais para a construção de um ambiente seguro e conforme com a LGPD. A sinergia entre a legislação, a governança de dados e a segurança da informação é crucial para a proteção dos direitos dos titulares de dados e para a mitigação dos riscos associados ao tratamento de dados pessoais.

O objetivo deste estudo é analisar os impactos da LGPD na segurança da informação dentro do setor de tecnologia da informação, com o intuito de identificar e avaliar as melhores práticas e políticas de segurança que assegurem a conformidade legal e protejam os dados pessoais contra acessos não autorizados, vazamentos e outras ameaças cibernéticas.

2 METODOLOGIA

De acordo com Gil (2010), trata-se de um estudo com objetivo descritivo e de abordagem qualitativa, pois foi concebido por intermédio de uma revisão bibliográfica de caráter narrativa para aprofundamento de quatro contextos, definidores das palavras-chave: Lei Geral de Proteção de Dados, Segurança da Informação, Gerenciamento de Riscos, Políticas de Segurança e Impacto Organizacional. Os descritores surgiram com o intuito de buscar as melhores fontes para o desenvolvimento da temática.

A base de dados indexados disponibilizada na internet para a busca do material bibliográfico foi o Google Acadêmico, um sistema de buscas refinadas do Google que oferece ferramentas de buscas de diversas fontes acadêmico-científicas. Também foram consultados e trazidos para a concepção do trabalho os principais referenciais teóricos em livros que abordavam as necessidades estabelecidas no objetivo do trabalho.

Durante o levantamento do material bibliográfico, tornou-se necessário estabelecer critérios de inclusão e exclusão destes para o processo de desenvolvimento textual. Os critérios de inclusão permitiram a participação de textos originais (artigos científicos, trabalhos monográficos, dissertação de mestrado e tese de doutorado) baseados em estudos de casos, escritos na língua portuguesa e sem determinação de período da publicação sobre a temática da LGPD e segurança da informação. Os critérios de exclusão consideraram a não relação com a temática da pesquisa e

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

inconsistências de qualidade e evidências técnicas, evitando-se a elaboração de um trabalho conceitual apenas,

A estratégia da revisão bibliográfica foi totalmente atrelada ao objetivo do estudo. Os processos de identificação e triagem foram realizados em conjunto com os autores e orientadores, para que a discussão avançasse no sentido de reconhecer com mais objetividade e agilidade os materiais que se adequassem ao tema.

3 REFERENCIAL TEÓRICO

O advento da LGPD no Brasil representa uma transformação significativa na forma como organizações lidam com dados pessoais. Conforme já apresentado, esta legislação estabelece um marco regulatório robusto para a proteção de informações pessoais, exigindo das empresas a adoção de medidas rigorosas de segurança da informação para garantir a privacidade e os direitos dos titulares dos dados.

No contexto da TI, a LGPD impõe desafios e oportunidades, obrigando os profissionais da área a revisitar e aprimorar suas práticas de gestão de dados e segurança cibernética. A implementação de políticas de conformidade, aliada ao desenvolvimento de tecnologias de proteção e monitoramento de dados, torna-se essencial para assegurar a integridade, confidencialidade e disponibilidade das informações, alinhando-se às exigências legais e fortalecendo a confiança dos usuários.

Este referencial teórico visa explorar os principais aspectos da LGPD, suas implicações na segurança da informação e as estratégias que as organizações de TI devem adotar para alcançar a conformidade e mitigar riscos associados à proteção de dados.

3.1 Aspectos Históricos de Fundamentação da LGPD no Brasil

A evolução da legislação de proteção de dados no Brasil reflete um crescente reconhecimento da importância da privacidade e da segurança da informação no cenário digital. A trajetória começa com a Constituição Federal de 1988, que, em seu artigo 5º, inciso X, assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. No entanto, a falta de uma regulamentação específica deixava lacunas significativas na proteção de dados pessoais, limitando a eficácia da tutela jurídica nesse campo (ALVES, 2023).

Um marco significativo na proteção de dados no Brasil ocorreu em 2014, com a promulgação do Marco Civil da Internet (Lei nº 12.965/2014). Esta legislação estabeleceu princípios, garantias, direitos e deveres para o uso da internet no país, incluindo disposições sobre a proteção de dados pessoais. O Marco Civil criou uma base para futuras regulamentações ao estabelecer diretrizes sobre a coleta, armazenamento, tratamento e uso de dados pessoais por provedores de internet, promovendo a transparência e a responsabilidade no ambiente digital.

A promulgação da LGPD em 2018 representou um avanço decisivo e abrangente na legislação de proteção de dados no Brasil. Inspirada na Regulamentação Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD trouxe um conjunto detalhado

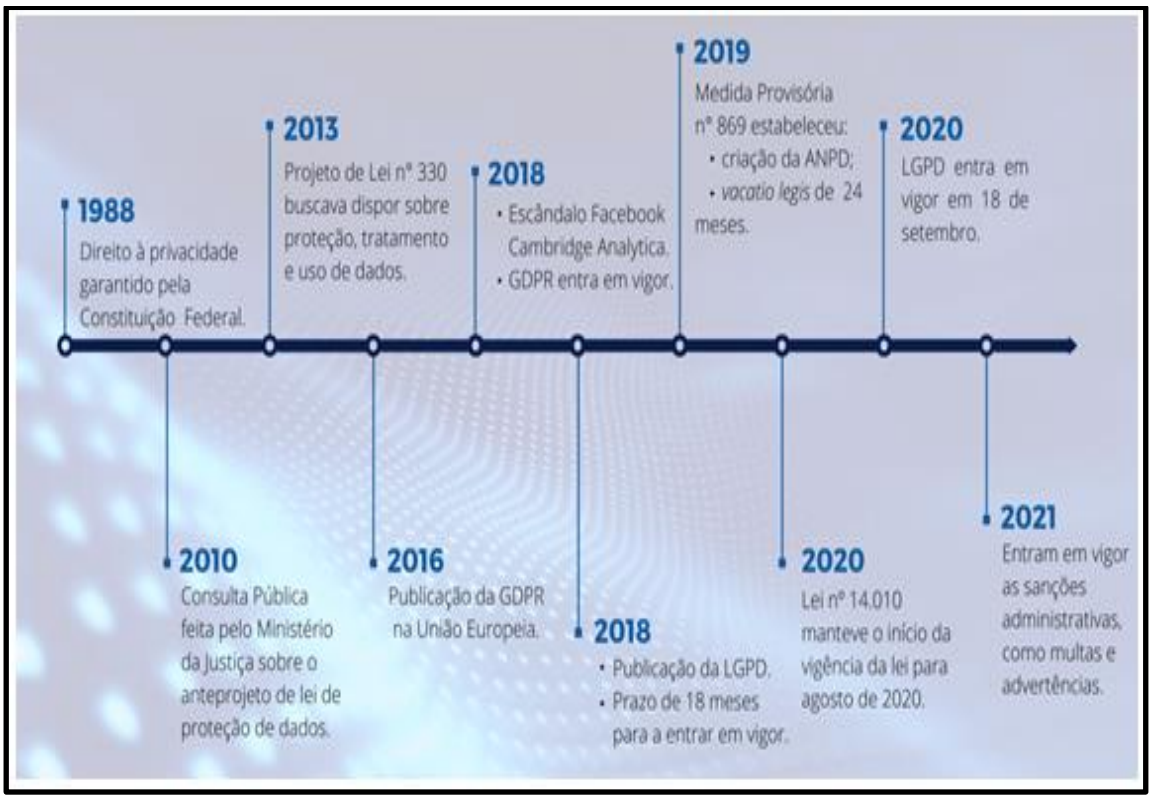
PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

de regras que regulamentam o tratamento de dados pessoais em qualquer setor da economia. Entrando em vigor em agosto de 2020, a LGPD estabeleceu direitos aos titulares de dados, definiu responsabilidades para controladores e processadores de dados, e criou a Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar e garantir o cumprimento da lei. Com isso, o Brasil se alinhou às melhores práticas internacionais, promovendo uma cultura de privacidade e proteção de dados que fortalece a confiança no ambiente digital e protege os direitos fundamentais dos cidadãos.

A **Figura 1** estabelece uma linha do tempo que resulta na implantação da LGPD no Brasil:

Figura 1. Linha do tempo de implantação da LGPD no Brasil.



Fonte: adaptado de *P&B – Privacy and Business Compliance*[1].

A **Figura 1** considera o referencial trazido na introdução deste trabalho (BRASIL, 2018; BRASIL, 2019, UNIÃO EUROPEIA, 2016). A LGPD e a Constituição Federal de 1988 estão intrinsecamente ligadas na promoção e proteção dos direitos fundamentais dos cidadãos brasileiros. Em seu artigo 5º, inciso X, a Constituição Brasileira assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, estabelecendo um direito à privacidade que serve como base para a proteção de dados pessoais. Este direito constitucional é ampliado pela LGPD, que detalha os mecanismos e

[1] Disponível em: https://encurtador.com.br/b1yaj

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

obrigações específicos para o tratamento adequado dos dados pessoais, refletindo uma evolução legislativa necessária para lidar com os desafios do mundo digital contemporâneo.

Em 2010, o Ministério da Justiça do Brasil lançou uma consulta pública sobre o anteprojeto de lei de proteção de dados pessoais, marcando um passo inicial significativo na formação de uma legislação dedicada à privacidade e segurança de informações no país. Este processo de consulta visava envolver a sociedade civil, especialistas e diversas partes interessadas na discussão e construção de um marco regulatório que pudesse responder aos desafios emergentes da era digital. A iniciativa permitiu a coleta de contribuições e sugestões que foram fundamentais para moldar o futuro texto legal, demonstrando um compromisso com a transparência e a participação democrática na formulação de políticas públicas relacionadas à proteção de dados pessoais.

O Projeto de Lei nº 330/2013, também conhecido como "Marco Civil da Proteção de Dados Pessoais", representou uma das primeiras tentativas no Brasil de criar uma legislação abrangente para regular a proteção, tratamento e uso de dados pessoais (BRASIL, 2013). Proposto em 2013, o projeto visava estabelecer princípios, direitos e responsabilidades para o tratamento de informações pessoais por parte de entidades públicas e privadas. Embora não tenha sido aprovado na forma original, o debate em torno do PL 330/2013 contribuiu significativamente para a conscientização sobre a importância da proteção de dados e influenciou o desenvolvimento posterior da Lei Geral de Proteção de Dados (LGPD), sancionada em 2018.

Em 2016, a União Europeia (2016) promulgou a Regulamentação Geral sobre a Proteção de Dados (GDPR), representando um marco abrangente e inovador na legislação de proteção de dados em todo o mundo. A GDPR foi concebida como uma resposta às crescentes preocupações com a privacidade e segurança dos dados pessoais em um cenário digital em rápida evolução. Esta legislação unificada estabeleceu padrões rigorosos para a coleta, armazenamento, processamento e transferência de dados pessoais, visando proteger os direitos dos cidadãos da UE e garantir a conformidade das organizações que operam dentro do bloco. Com sua entrada em vigor em maio de 2018, a GDPR definiu um novo padrão global para a proteção de dados, influenciando e orientando a legislação em vários países ao redor do mundo.

O escândalo do *Facebook* e Cambridge Analytica, em 2018, abalou as bases da privacidade de dados e provocou uma onda de preocupação global sobre o uso ético das informações pessoais na era digital. Revelou-se que a consultoria política *Cambridge Analytica* obteve ilegalmente dados de cerca de 87 milhões de usuários do Facebook, utilizando-os para influenciar estrategicamente eleições e campanhas políticas em todo o mundo. Esse incidente expôs as vulnerabilidades das plataformas de mídia social em relação à proteção de dados e levantou questões críticas sobre o controle e a responsabilidade das empresas em relação às informações pessoais de seus usuários. O escândalo gerou uma série de debates sobre regulamentações mais rígidas de privacidade de dados e destacou a necessidade urgente de medidas eficazes

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

para garantir a segurança e a integridade das informações pessoais online (SATIRA, 2021).

De 2018 a 2021, a implantação da Lei Geral de Proteção de Dados (LGPD) no Brasil foi marcada por uma intensa atividade de adaptação e implementação por parte das organizações. Durante esse período, as empresas em todo o país se empenharam em ajustar suas práticas de coleta, armazenamento e tratamento de dados pessoais para estar em conformidade com os requisitos estabelecidos pela legislação. Esse processo envolveu a revisão de políticas internas, a implementação de medidas de segurança da informação, a nomeação de encarregados pela proteção de dados (DPOs) e a realização de treinamentos para funcionários. Além disso, a criação da Autoridade Nacional de Proteção de Dados (ANPD) e a definição de diretrizes regulatórias contribuíram para orientar e fiscalizar a aplicação da LGPD, consolidando um ambiente jurídico propício à proteção da privacidade e dos direitos dos titulares de dados no Brasil.

3.2 Segurança da Informação

A segurança da informação desempenha um papel crucial na proteção dos ativos digitais de uma organização, garantindo a confidencialidade, integridade e disponibilidade dos dados. Em um mundo cada vez mais interconectado e dependente da tecnologia, a importância da segurança da informação é ampliada, visto que os dados são um dos ativos mais valiosos e sensíveis de uma empresa. Os princípios básicos da segurança da informação, como a necessidade de acesso mínimo, autenticação robusta, criptografia de dados, monitoramento contínuo e plano de contingência, fornecem uma base sólida para proteger as informações contra ameaças internas e externas. Ao implementar e aderir a esses princípios, as organizações podem mitigar riscos, evitar violações de dados e preservar a confiança dos clientes e parceiros (MACHADO, 2014).

Os princípios básicos da segurança da informação - confidencialidade, integridade e disponibilidade - formam a base fundamental para garantir a proteção eficaz dos dados e sistemas de uma organização. A confidencialidade refere-se à garantia de que apenas pessoas autorizadas tenham acesso às informações, protegendo-as contra divulgação não autorizada. A integridade, por sua vez, assegura que os dados permaneçam precisos, íntegros e confiáveis, protegendo-os contra alterações não autorizadas ou corrupção. Já a disponibilidade diz respeito à garantia de que as informações estejam acessíveis quando necessário, assegurando que os usuários legítimos possam acessá-las e utilizá-las conforme exigido para suas atividades. Em conjunto, esses princípios são essenciais para a construção de um ambiente de segurança robusto que proteja os ativos de informação de uma organização contra ameaças internas e externas (ABNT, 2018).

Normas e padrões internacionais desempenham um papel fundamental na garantia da segurança da informação em organizações ao redor do mundo. Um exemplo proeminente é a ISO 27001, uma norma que estabelece requisitos para um sistema de gestão de segurança da informação (SGSI), fornecendo diretrizes abrangentes para a implementação, monitoramento, manutenção e melhoria contínua da segurança da

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

informação. Ao adotar a ISO 27001, as organizações podem fortalecer suas defesas contra ameaças cibernéticas, mitigar riscos de segurança e demonstrar comprometimento com a proteção dos ativos de informação, resultando em maior confiança por parte dos stakeholders e parceiros comerciais (ISO, 2013).

3.3 Impactos da LGPD na Área de Tecnologia da Informação

3.3.1 Adequação e Conformidade

A adequação e conformidade na área de Tecnologia da Informação (TI) referem-se ao processo pelo qual as organizações garantem que suas práticas, políticas e sistemas estejam alinhados com as regulamentações, padrões e melhores práticas relevantes (ISO, 2013). Isso envolve a avaliação e análise dos requisitos legais e regulatórios aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), o Regulamento Geral de Proteção de Dados (GDPR) e normas específicas do setor, e a implementação de medidas necessárias para atender a esses requisitos. A conformidade eficaz na área de TI é essencial para garantir a segurança, privacidade e integridade dos dados, bem como para mitigar riscos legais, financeiros e reputacionais associados ao não cumprimento das regulamentações.

3.3.2 Processos e Etapas de Adequação

A adequação à Lei Geral de Proteção de Dados (LGPD) envolve uma série de processos e etapas que as organizações devem seguir para garantir a conformidade com a legislação, conforme Araújo (2020). O fluxograma trazido no **Quadro 1** pode servir como um guia básico para organizações que estão buscando se adequar à LGPD e garantir a proteção adequada dos dados pessoais que processam.

Inicialmente, é essencial realizar uma avaliação abrangente dos dados pessoais coletados, armazenados e processados pela organização, identificando os pontos de vulnerabilidade e os riscos associados ao tratamento dessas informações. Em seguida, é necessário elaborar e implementar políticas e procedimentos internos que atendam aos requisitos da LGPD, incluindo a nomeação de um encarregado pela proteção de dados, a revisão e atualização de contratos com terceiros e a implementação de medidas técnicas e organizacionais de segurança da informação. Além disso, é fundamental promover a conscientização e o treinamento dos colaboradores sobre as práticas de proteção de dados e a importância da privacidade, garantindo uma cultura organizacional alinhada com os princípios da LGPD.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

Quadro 1. Fluxograma sobre os processos e etapas para adequação à LGPD.

1 Avaliação Inicial:

- Identificar as áreas de negócio afetadas pela LGPD.
- Realizar uma análise de lacunas para identificar as áreas que precisam ser ajustadas para estar em conformidade com a LGPD.
- Designar um responsável pela conformidade com a LGPD.

2 Mapeamento de Dados:

- Identificar os dados pessoais coletados, armazenados e processados pela organização.
- Documentar o fluxo de dados e identificar onde eles estão armazenados e como são processados.

3 Análise de Riscos:

- Avaliar os riscos associados ao processamento de dados pessoais.
- Identificar potenciais vulnerabilidades e ameaças à segurança dos dados.

4 Desenvolvimento de Políticas e Procedimentos:

- Desenvolver políticas e procedimentos internos para garantir a conformidade com a LGPD.
- Incluir políticas para a obtenção de consentimento, o exercício dos direitos dos titulares dos dados e o tratamento de incidentes de segurança de dados.

5 Implementação de Medidas de Segurança:

- Implementar medidas técnicas e organizacionais para garantir a segurança dos dados pessoais.
- Isso pode incluir a criptografia de dados, o controle de acesso, a anonimização de dados, entre outras medidas.

6 Treinamento e Conscientização:

- Fornecer treinamento adequado sobre as práticas de proteção de dados pessoais para todos os funcionários que lidam com esses dados.
- Promover a conscientização sobre a importância da LGPD e os direitos dos titulares dos dados.

7 Monitoramento e Revisão:

- Estabelecer um processo contínuo de monitoramento e revisão das práticas de proteção de dados.
- Realizar auditorias regulares para garantir a conformidade contínua com a LGPD e ajustar as políticas e procedimentos conforme necessário.

8 Resposta a Incidentes:

- Desenvolver um plano de resposta a incidentes para lidar com violações de dados pessoais, conforme exigido pela LGPD.
- Isso inclui a notificação adequada às autoridades e aos titulares dos dados, bem como a mitigação dos impactos da violação.

9 Avaliação de Conformidade:

- Realizar avaliações regulares de conformidade com a LGPD para garantir que todas as medidas necessárias estejam sendo implementadas e seguidas adequadamente.
- Documentar todas as atividades de conformidade para fins de auditoria e prestação de contas.

Fonte: adaptado de Araújo (2020).

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

3.3.3 Principais Desafios e Obstáculos Enfrentados Pelas Organizações

As organizações enfrentam uma série de desafios e obstáculos significativos ao buscarem a conformidade com a LGPD no Brasil. Um dos principais desafios reside na mudança cultural e organizacional necessária para promover uma cultura de privacidade e proteção de dados em toda a empresa. Isso requer a conscientização e o engajamento de todos os colaboradores, desde a alta administração até os funcionários operacionais, e a implementação de políticas e procedimentos claros para garantir o cumprimento das disposições da LGPD.

Alves e Neves (2021) explicam que as organizações enfrentam desafios técnicos, como a identificação e classificação de dados pessoais em seus sistemas e processos, bem como a implementação de medidas de segurança adequadas para proteger esses dados contra acessos não autorizados e incidentes de segurança cibernética. Outro desafio importante é a alocação de recursos adequados, incluindo investimentos em tecnologia, treinamento de pessoal e consultoria especializada, para garantir uma implementação eficaz e sustentável das medidas de conformidade com a LGPD.

A adaptação à LGPD representa um desafio multifacetado que exige o comprometimento e a colaboração de toda a organização, bem como o investimento em recursos e capacidades adequadas para garantir a proteção adequada dos dados pessoais e o cumprimento das exigências legais.

3.3.4 Gestão de Riscos

A identificação e mitigação de riscos relacionados à proteção de dados constituem um desafio fundamental para as organizações que buscam adequar-se à LGPD no Brasil. Nesse contexto, as empresas enfrentam uma série de ameaças, incluindo vazamento de informações, violações de segurança cibernética, uso inadequado de dados pessoais e falta de conformidade com os princípios e requisitos estabelecidos pela legislação. Para mitigar esses riscos, as organizações devem realizar uma avaliação abrangente de seu ecossistema de dados, identificando pontos vulneráveis e implementando medidas de segurança adequadas, como criptografia, autenticação multifatorial, políticas de acesso e controle de privilégios, além de treinamentos regulares para conscientização dos funcionários (LISBOA, 2021).

Além disso, é fundamental estabelecer processos claros de governança de dados, incluindo a nomeação de um Encarregado de Proteção de Dados (DPO) e a criação de políticas internas de proteção de dados que estejam alinhadas com os princípios e diretrizes estabelecidos pela LGPD. Essas medidas não apenas ajudam a reduzir os riscos de não conformidade e as consequentes sanções legais, mas também fortalecem a confiança dos clientes e parceiros, promovendo uma cultura de segurança e respeito à privacidade dos dados.

Desta forma, torna-se essencial que se faça uma “Análise de Impacto sobre a Proteção de Dados” (DPIA), que surge como uma ferramenta para as organizações enfrentarem os desafios de conformidade com a LGPD (SONEHARA; CASSIANO, 2020). Esta análise sistemática e detalhada permite às empresas identificar, avaliar e

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

mitigar os riscos associados ao tratamento de dados pessoais, alinhando suas práticas às exigências legais da LGPD. As organizações enfrentam uma série de desafios ao realizar DPIAs, incluindo: a) necessidade de compreender a complexidade de seus ecossistemas de dados, b) identificar e classificar dados pessoais; c) avaliar os impactos potenciais das atividades de tratamento de dados e; d) implementar medidas de proteção e segurança adequadas.

A realização de DPIAs de forma eficaz requer o envolvimento de múltiplas partes interessadas, incluindo equipes de TI, jurídico, conformidade e gestão de riscos, para garantir uma abordagem holística e abrangente à proteção de dados dentro da organização. Um DPIA geralmente segue várias etapas para garantir uma avaliação abrangente dos riscos e impactos relacionados ao tratamento de dados pessoais, conforme tem-se a seguir:

Etapa 1: Preparação e Escopo

- Definição dos objetivos da DPIA e escopo do projeto.
- Identificação das partes interessadas envolvidas no processo.
- Determinação dos critérios de avaliação e das métricas a serem utilizadas.

Etapa 2: Mapeamento de Dados

- Identificação e categorização dos dados pessoais coletados e processados pela organização.
- Análise da origem, fluxo e destino dos dados ao longo de seu ciclo de vida.
- Avaliação da sensibilidade e criticidade dos dados em relação aos direitos dos titulares.

Etapa 3: Avaliação de Riscos

- Identificação dos possíveis riscos e impactos associados ao tratamento de dados pessoais.
- Análise das ameaças à segurança, vulnerabilidades e probabilidade de ocorrência.
- Classificação e priorização dos riscos de acordo com sua gravidade e probabilidade de ocorrência.

Etapa 4: Avaliação da Necessidade e Proporcionalidade

- Avaliação da necessidade e proporcionalidade das atividades de tratamento de dados em relação aos objetivos organizacionais.
- Verificação da conformidade com os princípios da LGPD, como o princípio da finalidade, da adequação e da necessidade.

Etapa 5: Medidas de Mitigação e Controle

- Desenvolvimento de planos de ação para mitigar e controlar os riscos identificados.

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

- Implementação de medidas técnicas e organizacionais para reduzir os riscos à proteção de dados.
- Documentação das medidas adotadas e responsabilidades atribuídas.

Etapa 6: Revisão e Monitoramento

- Revisão contínua da DPIA para garantir sua relevância e eficácia ao longo do tempo.
- Monitoramento regular das atividades de tratamento de dados e dos controles implementados.
- Atualização da DPIA conforme necessário em resposta a mudanças nos processos, tecnologias ou regulamentações aplicáveis.

Quanto ao fluxo das etapas de desenvolvimento da DPIA é fundamental ressaltar a importância contínua deste processo na jornada de conformidade com a LGPD. A DPIA não é apenas uma obrigação legal, mas também uma ferramenta estratégica para garantir a proteção eficaz dos dados pessoais e a preservação da privacidade dos indivíduos. Ao realizar DPIAs de forma regular e sistemática, as organizações não apenas identificam e mitigam riscos, mas também promovem uma cultura de segurança da informação e transparência em suas operações. Portanto, ao incorporar a DPIA como parte integrante de suas práticas de governança de dados, as organizações demonstram seu compromisso com a proteção da privacidade e o cumprimento das leis e regulamentos de proteção de dados, fortalecendo a confiança de seus clientes e parceiros comerciais (SONEHARA; CASSIANO, 2020).

3.4 Implementação de Medidas de Segurança da Informação

3.4.1 Políticas e Procedimentos de Segurança

Políticas e procedimentos de segurança são diretrizes e práticas estabelecidas por uma organização para proteger seus ativos de informação contra ameaças internas e externas (CARLOTO, 2023). As políticas de segurança definem os princípios gerais e objetivos de segurança da informação, enquanto os procedimentos detalham as ações específicas a serem seguidas para implementar e manter essas políticas. Essas políticas e procedimentos abrangem uma variedade de áreas, como controle de acesso, gestão de identidade, criptografia, monitoramento de redes, backup e recuperação de dados, entre outros.

Ao estabelecer e aplicar políticas e procedimentos de segurança de forma consistente, as organizações podem reduzir o risco de incidentes de segurança, proteger a confidencialidade, integridade e disponibilidade de seus dados e sistemas, e demonstrar conformidade com regulamentos e padrões de segurança aplicáveis (CARLOTO, 2023).

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

3.4.2 Implementação de Políticas e Procedimentos de Segurança

Pedrosa (2021) enfatiza que a implementação de políticas e procedimentos de segurança nas organizações é um processo abrangente que envolve várias etapas e considerações importantes. Primeiramente, é essencial que a alta administração demonstre um forte comprometimento com a segurança da informação, estabelecendo uma cultura organizacional que valorize a proteção dos dados. Em seguida, as políticas de segurança devem ser desenvolvidas de forma clara, abrangente e alinhadas aos objetivos estratégicos da organização, considerando os requisitos regulatórios, as melhores práticas do setor e os riscos específicos enfrentados pela empresa. Essas políticas devem abordar aspectos como controle de acesso, uso adequado de sistemas e recursos de informação, classificação e tratamento de dados sensíveis, gestão de incidentes de segurança, entre outros.

Após a definição das políticas, é fundamental comunicá-las de maneira eficaz a todos os colaboradores, fornecendo treinamentos e conscientização sobre as práticas de segurança e as responsabilidades individuais de cada membro da equipe. Além disso, é necessário estabelecer procedimentos operacionais claros e documentados para garantir a aplicação consistente das políticas de segurança no dia-a-dia das operações da organização. Isso pode incluir a implementação de controles técnicos, como firewalls, antivírus, criptografia e autenticação multifator, bem como processos de monitoramento e auditoria para detectar e responder a possíveis violações de segurança (PEDROSA, 2021).

Por fim, a implementação bem-sucedida das políticas e procedimentos de segurança requer uma abordagem contínua de avaliação e melhoria, por meio de revisões regulares das políticas, análises de risco periódicas, testes de vulnerabilidade e incidentes simulados. Essa abordagem iterativa permite que as organizações adaptem suas práticas de segurança às mudanças no ambiente de ameaças e aos novos requisitos de negócios, garantindo assim a proteção contínua dos ativos de informação e a mitigação eficaz dos riscos de segurança (PEDROSA, 2021).

O **Quadro 2** apresenta as fases de implementação das Políticas e Procedimentos de Segurança nas organizações:

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

Quadro 2. Fases de implementação das Políticas e Procedimentos de Segurança.

Fase de Planejamento: a organização define suas políticas de segurança, estabelecendo diretrizes gerais para proteger os ativos de informação e mitigar riscos de segurança cibernética.
Fase de Desenvolvimento: são elaborados os procedimentos operacionais específicos, incluindo controles de acesso, criptografia de dados, políticas de senhas, entre outros, de acordo com as políticas de segurança estabelecidas.
Fase de Implementação: as políticas e procedimentos de segurança são comunicados a todos os funcionários e partes interessadas relevantes, e são implantados sistemas e ferramentas de segurança necessários para garantir a conformidade e eficácia das medidas de segurança.
Fase de Treinamento e Conscientização: os funcionários são capacitados sobre as políticas e procedimentos de segurança, e são alertados sobre práticas seguras de uso de sistemas e dados. Este treinamento é essencial para garantir que todos os membros da organização compreendam a importância da segurança da informação e saibam como agir corretamente em caso de incidentes de segurança.
Fase de Monitoramento e Avaliação: a organização realiza auditorias de segurança regulares para garantir a conformidade contínua com as políticas e procedimentos de segurança, e para identificar áreas de melhoria.

Fonte: elaborado pelos autores.

O *feedback* obtido durante esse processo é utilizado para ajustar e atualizar as políticas e procedimentos de segurança conforme necessário, garantindo que a organização permaneça resiliente e protegida contra ameaças cibernéticas em constante evolução. Este ciclo de implementação contínua e melhoria contínua é fundamental para manter um ambiente de segurança robusto e adaptável às mudanças no cenário de ameaças de segurança.

3.4.3 Tecnologias e Ferramentas

Existem diversas ferramentas e tecnologias disponíveis para proteção de dados e segurança da informação, cada uma desempenhando um papel específico na mitigação de riscos cibernéticos e na garantia da confidencialidade, integridade e disponibilidade dos dados. Entre as principais ferramentas destacam-se, segundo Barbosa et al. (2021):

- ***Firewalls:*** utilizados para monitorar e controlar o tráfego de rede, permitindo ou bloqueando o acesso com base em políticas de segurança predefinidas.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

- **Antivírus e *Antimalware*:** ferramentas projetadas para detectar, prevenir e remover ameaças de software malicioso, como vírus, *worms*, trojans, entre outros.
- **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS):** monitoram e analisam o tráfego de rede em busca de atividades suspeitas ou comportamentos maliciosos, podendo alertar ou bloquear ataques em tempo real.
- **Controle de Acesso e Gerenciamento de Identidade (IAM):** permitem definir e gerenciar permissões de acesso dos usuários aos recursos da organização, garantindo que apenas pessoas autorizadas tenham acesso a dados sensíveis.
- **Criptografia:** técnica que codifica dados para que só possam ser lidos por pessoas autorizadas, protegendo informações confidenciais durante o armazenamento, transmissão e processamento.
- ***Backup* e Recuperação de Dados:** ferramentas e processos para realizar cópias de segurança dos dados e garantir sua recuperação em caso de falhas, ataques cibernéticos ou desastres.
- **Monitoramento de Segurança e Análise de Logs:** ferramentas que registram e analisam atividades de sistema e de rede para identificar possíveis incidentes de segurança, detectar padrões anômalos e apoiar investigações forenses.
- **Proteção de *Endpoints*:** soluções projetadas para proteger dispositivos finais, como computadores, smartphones e tablets, contra ameaças de segurança, incluindo antivírus, firewall pessoal e prevenção contra roubo de dados.
- **Gestão de Vulnerabilidades:** ferramentas que escaneiam e identificam vulnerabilidades em sistemas e redes, permitindo que as organizações priorizem e corrijam essas falhas de segurança.
- **Treinamento de Conscientização em Segurança:** não é uma ferramenta tecnológica, mas é fundamental para educar os funcionários sobre práticas de segurança da informação, prevenção de ataques de *phishing*, engenharia social e outros riscos cibernéticos.

Essas são apenas algumas das ferramentas e tecnologias disponíveis para proteger dados e garantir a segurança da informação em ambientes corporativos. A escolha e implementação adequadas dessas ferramentas devem ser guiadas por uma avaliação abrangente de riscos e pela aderência às regulamentações de segurança pertinentes.

3.4.4 Monitoramento e Resposta a Incidentes de Segurança

O monitoramento e resposta a incidentes de segurança é uma prática fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados em uma organização (FERRAZ, 2021). Para realizar esse processo de forma eficaz, é necessário seguir algumas etapas-chave. Primeiramente, é essencial estabelecer um sistema de monitoramento contínuo da rede, sistemas e aplicativos, utilizando ferramentas de segurança como firewalls, sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS). Essas ferramentas ajudam a identificar atividades suspeitas ou potencialmente maliciosas.

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

Em seguida, é importante ter procedimentos claros e bem definidos para lidar com incidentes de segurança. Isso inclui a criação de um plano de resposta a incidentes que detalha as etapas a serem seguidas quando uma violação de segurança é detectada. Esse plano deve incluir a designação de responsabilidades específicas para membros da equipe, a definição de protocolos de comunicação interna e externa e a documentação de evidências para investigações futuras (FERRAZ, 2021).

Além disso, é importante realizar treinamentos regulares para toda a equipe, a fim de aumentar a conscientização sobre segurança da informação e garantir que todos saibam como reconhecer e relatar incidentes de segurança. A análise pós-incidente também é uma etapa importante, permitindo à organização aprender com os incidentes passados e fazer melhorias contínuas em seus processos de segurança. Em resumo, o monitoramento e resposta a incidentes de segurança requerem uma abordagem proativa, multidisciplinar e em constante evolução para proteger os ativos de informação de uma organização contra ameaças cibernéticas.

4 RESULTADOS

Como resultado deste estudo teórico, buscou análises práticas de estudos de caso. As análises práticas de estudos de caso representam uma abordagem metodológica valiosa para compreender a aplicação real da LGPD nas organizações. Mesmo com a apresentação breve dos casos, permite identificar melhores práticas, avaliar a eficácia das políticas de proteção de dados e entender as nuances contextuais que influenciam o sucesso ou fracasso das iniciativas de segurança da informação.

4.1 Estudo de Caso 1: Sucesso na Implemento da LGPD

Um exemplo de empresa que implementou com sucesso a LGPD e medidas robustas de segurança da informação é a Nubank, uma *fintech* brasileira conhecida por sua inovação e foco na experiência do cliente (FALCÃO, 2022). Desde o início de suas operações, o Nubank tem adotado uma abordagem proativa para a proteção de dados pessoais e a conformidade com as regulamentações aplicáveis. A empresa investiu significativamente em tecnologias avançadas de segurança da informação, como criptografia de ponta a ponta, autenticação multifatorial e monitoramento contínuo de ameaças cibernéticas.

A Nubank estabeleceu políticas e procedimentos claros para o tratamento responsável de dados dos clientes, incluindo a realização de Avaliações de Impacto sobre a Proteção de Dados (DPIAs) e a designação de um Encarregado de Proteção de Dados (DPO) para supervisionar questões relacionadas à privacidade. Como resultado dessas medidas, a Nubank construiu uma reputação sólida de confiança e segurança entre seus milhões de clientes, demonstrando que é possível conciliar inovação tecnológica com proteção eficaz de dados pessoais.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

4.2 Estudo de Caso 2: **Problemas por Falta de Conformidade com a LGPD**

Trata-se de uma organização fictícia que enfrentou problemas significativos devido à falta de conformidade com a Lei Geral de Proteção de Dados (LGPD). Seria uma empresa de tecnologia de médio porte que operava no setor de comércio eletrônico. Antes da entrada em vigor da LGPD, a empresa coletava uma ampla gama de dados pessoais de seus clientes sem o devido consentimento ou transparência sobre como esses dados seriam usados. Além disso, as medidas de segurança da informação eram insuficientes, deixando os dados dos clientes vulneráveis a violações de segurança.

Com a implementação da LGPD, a empresa se viu obrigada a realizar uma revisão abrangente de suas práticas de proteção de dados. Isso incluiu a nomeação de um Encarregado de Proteção de Dados (DPO) e a realização de uma Análise de Impacto sobre a Proteção de Dados (DPIA) para identificar e avaliar os riscos associados ao tratamento de dados pessoais. No entanto, a falta de processos e controles adequados tornou a empresa incapaz de lidar eficazmente com as exigências da LGPD.

Como resultado, a empresa enfrentou várias consequências adversas. Além de multas significativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) devido à não conformidade com a LGPD, houve também danos à reputação da empresa e perda de confiança por parte dos clientes. Essa situação destacou a importância crítica da conformidade com a LGPD e serviu como um alerta para outras organizações sobre a necessidade de adotar práticas sólidas de proteção de dados para evitar consequências graves.

4.3 Análise Crítica dos Casos

A análise crítica dos casos estudados revela uma variedade de boas práticas e erros comuns cometidos pelas organizações em relação à proteção de dados. Entre as boas práticas observadas está a implementação de políticas de privacidade claras e acessíveis, que informam os titulares de dados sobre como suas informações serão utilizadas e protegidas. Além disso, a adoção de medidas técnicas e organizacionais robustas, como a criptografia de dados e a pseudonimização, demonstrou um compromisso efetivo com a segurança da informação e a conformidade com os requisitos da LGPD.

Por outro lado, erros comuns incluem a falta de transparência na coleta e uso de dados pessoais, resultando em falta de confiança dos usuários e potenciais violações da legislação. Além disso, a negligência na implementação de medidas de segurança adequadas, como firewalls e sistemas de detecção de intrusões, expõe as organizações a riscos significativos de violação de dados e danos à reputação.

A análise crítica destaca a importância de uma abordagem proativa e holística para a proteção de dados, que engloba políticas claras, medidas de segurança robustas e uma cultura organizacional centrada na privacidade e na conformidade legal.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.12718309 Artigo de Revisão

5 CONSIDERAÇÕES FINAIS

O presente trabalho oferece uma análise detalhada sobre a importância da LGPD no contexto da tecnologia da informação, destacando os desafios enfrentados pelas organizações para se adequarem às suas exigências. Por meio de uma revisão abrangente da legislação, foram identificados os principais pilares da LGPD, como a proteção dos direitos dos titulares de dados, a necessidade de consentimento para o tratamento de informações pessoais e a responsabilidade das empresas em garantir a segurança e privacidade dos dados. Além disso, foram discutidas as implicações práticas da LGPD para as organizações, incluindo a realização de análises de impacto sobre a proteção de dados (DPIA) e a implementação de medidas de segurança da informação.

Acredita-se que o estudo contribuiu para a área de tecnologia da informação ao fornecer uma visão abrangente dos desafios e oportunidades apresentados pela LGPD. Ao destacar a importância da proteção de dados e a necessidade de conformidade com a legislação, o trabalho destaca a relevância de uma abordagem proativa na gestão da segurança da informação e na governança de dados. Além disso, ao discutir a realização de DPIAs e a implementação de medidas de segurança, o estudo oferece orientações práticas para as organizações que buscam garantir a conformidade com a LGPD e fortalecer a proteção de dados em seus ambientes digitais.

Para pesquisas futuras, sugere-se a realização de estudos mais aprofundados sobre a eficácia das medidas de segurança da informação na proteção de dados pessoais em diferentes contextos organizacionais. Além disso, é importante investigar os impactos econômicos e sociais da LGPD, incluindo os custos associados à conformidade e os benefícios decorrentes da proteção de dados para os titulares de dados e para a sociedade em geral. Outra área promissora para pesquisa é a análise do papel das tecnologias emergentes, como inteligência artificial e *blockchain*, na proteção de dados e na conformidade com a legislação de privacidade, explorando seu potencial para melhorar a segurança e a transparência no tratamento de informações pessoais.

REFERÊNCIAS

ALVES, P. H. S. **A evolução da legislação de proteção de dados pessoais no Brasil.** 2024. Disponível em: < https://encurtador.com.br/rozwB L>. Acesso em: 14 jun. 2024.]

ALVES, C.; NEVES, M. **Especificação de Requisitos de Privacidade em Conformidade com a LGPD:** Resultados de um Estudo de Caso. 2021. Disponível em: https://encurtador.com.br/H4k1p. Acesso em: 14 jun. 2024.

ARAÚJO, P. P. P. **Adequação à LGPD:** Processos e Etapas. São Paulo: Saraiva Educação, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Conformidade com a Lei Geral de Proteção de Dados (LGPD):** Desafios e Estratégias para Organizações. Relatório. Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS Técnicas (ABNT). (2018). **NBR ISO/IEC 27002:2013** - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT.

DOI: 10.5281/zenodo.12718309 *Artigo de Revisão*

BARBOSA, J. S. et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557-e40510212557, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), e o Decreto-Lei nº 5.462, de 1º de maio de 1943 (Consolidação das Leis do Trabalho - CLT). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Seção 1, p. 1.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Dispõe sobre a criação da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, DF, 9 jul. 2019. Seção 1, p. 1.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 330, de 2013.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF, 2013.

CARLOTO, S. **Lei Geral da Proteção de Dados:** Incluindo Modelos, Segurança da Informação e Fases de Implementação.4ª ed. São Paulo: LTr Editora, 2023.

FALCÃO, J. D. F**. Os desafios dos bancos frente ao surgimento das fintechs no Brasil:** um estudo de caso do Inter e Nubank. 2023. 50 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Econômicas) - Faculdade de Economia, Administração e Contabilidade, Universidade Federal de Alagoas, Maceió, 2022.

FERRAZ, J. T. Plano de resposta a incidentes de segurança. **Cadernos Jurídicos da Faculdade de Direito de Sorocaba**, v. *3*, n. 1, p. 121–141, 2022.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 5. ed. São Paulo: Atlas, 2010.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001:2013.** Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos. Genebra, Suíça: ISO, 2013.

LISBOA, L. R. **Gestão de riscos em segurança da informação.** Monografia (Trabalho de Conclusão de Curso em Ciência da Computação) - Universidade Feevale, 2021.

MACHADO, F. N. R. **Segurança da Informação:** Princípios e controle de ameaças. São Paulo: Saraiva, 2014.

PEDROSA, J. A. L. **Segurança da Informação:** Auditorias, Implementação de Medidas de Segurança e de Conformidade em Empresas. Dissertação (Mestrado em Cibersegurança e Informática Forense) - Escola Superior de Tecnologia e Gestão, Leiria, Portugal, 2021.

SATIRA, R. **O maior escândalo de "vazamento" de dados**: o caso Facebook - *Cambridge Analytica*, e a importância da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. 2021. Disponível em: https://encurtador.com.br/TlzRg. Acesso em: 14 jun. 2024.

SILVA, J. A**. Segurança da Informação e LGPD:** Desafios e Perspectivas. São Paulo: Editora Tecnologia Avançada, 2022.

SONEHARA, I. M., CASSIANO, L. G. S. **Análise de impacto na proteção de dados**, 2020. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2020

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas: União Europeia, 2016.

Os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.