Recomendações para Conformidade com a LGPD a partir de uma Revisão Sistemática da Literatura

Gabriel da S. Belarmino[1],**Gustavo H. M. B. Motta**[1], **Danielle R. D. Ricarte** [1], **Luiz Fernando F. P. de Lima** [2]

[1]Universidade Federal da Paraíba - João Pessoa- PB - Brasil.

[2]CESAR - Recife - PE - Brasil.

gabriel.belarmino@academico.ufpb.br, danielle@ci.ufpb.br,

gustavo@ci.ufpb.br, lffpl@cesar.org.br.

Resumo. *O avanço da informatização e do desenvolvimento tecnológico gerou a evolução na manipulação e transferência de dados. Essa evolução, promove preocupações crescentes quanto à segurança e proteção de dados pessoais, culminando na criação da nova legislação, a Lei Geral de Proteção de Dados (LGPD) brasileira. Executando uma revisão da literatura, este artigo coleta artefatos relacionados aos processos organizacionais que são úteis para promover a conformidade com a LGPD e a regulamentação europeia, a fim de desenvolver recomendações técnicas de privacidade. A análise e correlação dos diferentes artefatos coletados permitiram a sugestão de sete recomendações para executar processos de privacidade eficientes para a LGPD.*

Palavras chave*: LGPD, RGPD, segurança da informação, dados pessoais, conformidade, processos organizacionais*

Abstract. *The advancement of computerization and technological development has led to the evolution of data manipulation and transfer. This evolution has raised growing concerns regarding the security and protection of personal data, culminating in the creation of new legislation, the Brazilian General Data Protection Law (LGPD). Through a literature review, this article gathers artifacts related to organizational processes that are useful for promoting compliance with the LGPD and European regulations, in order to develop technical privacy recommendations. The analysis and correlation of the different collected artifacts have enabled the formulation of seven recommendations for executing efficient privacy processes for the LGPD.*

keywords*: LGPD, GDPR, information security, personal data, compliance, organizational process*

1. Introdução

A informatização de processos do cotidiano como comércio eletrônico, redes sociais, aplicativos bancários, dentre outras ferramentas modernas, resultou em uma significativa geração de informações pessoais e de clientes. Esses dados se tornaram ativos essenciais para empresas, órgãos governamentais e governos, conferindo maior poder econômico

às organizações detentoras de grandes volumes de dados. Porém, essa relevância traz consigo implicações para a sociedade, pois a deixa mais exposta à falhas de segurança, ataques cibernéticos, roubo e venda de informações pessoais e publicidades indevidas [Lopes and Amaral 2022].

Mediante isso, surgiu a Lei Geral de Proteção de Dados (LGPD) [LGPD 2018] inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) europeu [GDPR 2016]. Ambos os regulamentos compartilham objetivos semelhantes ao estabelecerem regras para fortalecer os direitos de privacidade e a segurança das informações. Embora muitos requisitos técnicos da LGPD sejam análogos aos da lei europeia, houve adaptações legislativas e territoriais específicas na legislação brasileira.

O escopo do regimento brasileiro é salvaguardar a forma de tratar dados pessoais, garantindo que direitos essenciais de liberdade e o desenvolvimento do cidadão sejam promovidos. A LGPD abrange todas as operações no Brasil que envolvem dados individuais, não se limitando ao âmbito digital, mas englobando todo tipo de tratamento realizado por organizações públicas e privadas no país [Okano et al. 2021].

Diante desse cenário, a LGPD demanda adaptações profundas para os órgãos nacionais que lidam com dados pessoais. Inúmeros ajustes são requeridos para atender às exigências do regulamento, o qual prevê sanções e multas para organizações que não estejam em conformidade. Apesar de discussões e investimentos em curso, muitas organizações no Brasil e globalmente ainda não completaram integralmente as mudanças necessárias.

Uma pesquisa nacional realizada entre 2022 e 2023 pelo IDESP (Instituto Daryus de Ensino Superior Paulista) [Daryus 2023], indicou que 80% das organizações no Brasil estão em processo de adaptação à LGPD. Cerca de 55% delas afirmam ter cumprido pelo menos 70% das exigências, enquanto 21% ainda não iniciaram ou não possuem informações sobre esse processo. Esses números ressaltam a complexidade e a relevância da transição para a conformidade com LGPD em contexto empresarial e institucional em constante evolução.

Tanto a comunidade científica quanto organizações públicas e as empresas privadas estão em busca de procedimentos adequados e soluções teóricas e práticas para implementar os novos regulamentos de privacidade de dados para lidar com as problemáticas de conformidade. Uma das maiores vulnerabilidades identificadas nas organizações está relacionada à "Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação" [Daoudagh and Marchetti 2022].

A área de Tecnologia da Informação (TI) desempenha um papel crucial na implementação e execução da LGPD ao garantir a segurança das informações dos usuários. Dessa forma, é necessário avaliar quais impactos refletidos nos processos organizacionais, e quais as soluções propostas para desenvolver metodologias eficientes associadas às técnicas de Tecnologia e Segurança da Informação na proteção de dados pessoais, por exemplo, quais serão os processos humanos, institucionais e culturais carecidos de transformações.

Este trabalho realiza uma revisão sistemática com o objetivo de analisar a conjuntura das principais soluções encontradas para implementar as demandas da LGPD nos processos organizacionais das instituições brasileiras. Além disso, são consideradas al-

gumas soluções presentes no RGPD europeu que possuem contexto e aplicação semelhantes ao da legislação nacional. Como contribuições, a pesquisa apresenta propostas de recomendações, intervenções e estratégias de implementação concretas para a conformidade com a legislação, sob a perspectiva da Gestão de Dados e da SI.

Em sua estrutura, o presente artigo apresenta na Seção 2, as especificações das legislações de proteção de dados e dos temas relacionados para sua compreensão e finalidade. Nas Seções 3 e 4 são apresentados estudos relacionados e a metodologia empregada de revisão sistemática, respectivamente. Como resultados, nas seções 5 e 6 são expostas as análises dos estudos coletados e recomendações de proteção de dados. Por fim, a Seção 7 descreve as conclusões e define trabalhos futuros.

2. Fundamentação Teórica

Nesta seção, são apresentados os fundamentos para compreensão do objeto de pesquisa. Inicia-se pela abordagem conceitual dos dados pessoais, delineando sua importância como o cerne das novas legislações. São exploradas as operações que envolvem os dados, destacando sua relevância e variedade de usos. Em seguida, é oferecida uma descrição tanto do RGPD europeu quanto da LGPD brasileira. Essas legislações representam marcos cruciais na proteção e regulação do tratamento de informações pessoais, sendo essenciais para o entendimento do escopo e das exigências legais que moldam o contexto desta pesquisa.

2.1. Privacidade de Dados

No meio organizacional e nos ambientes digitais, o compartilhamento e manipulação de dados de indivíduos ocorre frequentemente. Os dados dos indivíduos são intitulados de dados pessoais, e representam informações, fatos, interesses e relações que se referem a uma pessoa identificável [Montolli 2020]. Exemplos de dados pessoais comuns são: nome, CPF, telefone, ocupação profissional e histórico de saúde. É relevante expressar que os dados (como dados pessoais) não são informações propriamente, i.e., isoladamente dados são apenas registros sem significado.

Uma categoria de dados pessoais cada vez mais importantes para empresas e para a sociedade são os dados pessoais sensíveis. Tais dados geram atenção, pois caracterizam dados de caráter privado, já que são capazes de gerar informações sensíveis sobre os cidadãos. Os dados estão geralmente relacionados com questões que envolvem saúde, origem racial ou étnica, direcionamento político, religiosidade, orientação sexual, identidade de gênero, dentre outros da mesma natureza [Montolli 2020].

As operações realizadas com estes dados são recorrentemente denominadas de 'tratamento de dados'. O tratamento simboliza quaisquer ações realizadas com o dado obtido, e podem ser listadas como: coleta, produção, compartilhamento, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, comunicação, entre outras [Paini and Zilles 2021].

O termo privacidade é utilizado para aspectos diversificados, dependendo da área em estudo. Neste trabalho, consideramos que a privacidade de dados pessoais é o direito do indivíduo de manter suas informações resguardadas, sem interferência de outras pessoas ou entidades [Lima 2020].

A preocupação com a privacidade de dados pessoais cresce a cada ano, graças à evolução da TI. O cumprimento deste direito encontra muitos desafios e barreiras com a alta distribuição, compartilhamento e fluxo de informações. Logo, do ponto de vista técnico, é prioritário alinhar sistemas e tecnologias da informação, protegendo e privando os dados que gerenciam. No âmbito administrativo, normas como ISO/IEC 27701 [ISO/IEC 2019] e ISO/IEC 27002 [ISO/IEC 2022] formalizam procedimentos para melhorar práticas e garantir a preservação nos dados [Ferrão et al. 2021].

2.2. Governança de Dados

A Governança é um conceito usado no ambiente organizacional, para descrever ações relacionadas à tomada de decisão coletiva e coordenada por indivíduos que trabalham em conjunto, atuando em atividades de interesse para toda a organização. Já a Governança de Dados, é um tipo de gestão de informação que observa a utilização de dados de forma estratégica e planejada, para estruturar a forma de coleta, armazenamento e tratamentos executados na organização [Montolli 2020].

Essa gestão é importante pois, a partir da governança de dados, é possível visualizar as informações manipuladas como fontes valiosas para traçar estratégias e exercer o controle sobre o gerenciamento de dados nos processos organizacionais. As atividades previstas nesse domínio estão relacionadas a desenvolver políticas, padrões e processos capazes de garantir a segurança, integridade e disponibilidade dos dados [Silva 2021].

2.3. Segurança da Informação

A Segurança da Informação (SI) aliada a privacidade e a Governança de Dados são temáticas em evidência, devido a grande quantidade de dados corporativos processados e distribuídos na internet e em sistemas de informação. Em adição, os perigos de incidentes e de ataques nas informações organizacionais e pessoais estão cada vez maiores [Montolli 2020]. A SI pode ser definida como a proteção a sistemas de informação, objetivando preservar a integridade, a confidencialidade e a disponibilidade de recursos do sistema, os três pilares da Segurança da Informação [Lima 2020].

Para a SI, a informação é um ativo valioso que precisa ser protegido e, se possível, aprimorado utilizando normas e medidas técnicas explicitadas nas políticas de segurança. Tais políticas visam minimizar qualquer dano de segurança e manter a continuidade estável das atividades corporativas [ROCHA et al. 2019]. Exemplos de ativos de informação considerados pela SI são equipamentos, usuários, bases de dados e sistemas. Além de seus requisitos tradicionais, atualmente a SI também deve se adequar às questões societárias e regulatórias, os novos regulamentos que influenciam neste contexto são apresentados a seguir.

2.4. RGPD

Em vigor desde 25 de maio de 2018, o RGPD representa uma das mudanças mais significativas das últimas décadas no contexto da proteção de dados pessoais. Destacando-se como uma iniciativa pioneira, o RGPD estabeleceu um conjunto qualificado de normas, ampliando consideravelmente as regras e diretrizes referentes à privacidade de dados. Este regulamento impõe obrigações legais específicas para os órgãos responsáveis pelo processamento de informações pessoais.

Dentre os principais avanços gerados pela lei, destaca-se a definição de diretrizes para operações no ambiente digital. Essas diretrizes incluem o reconhecimento do direito ao esquecimento, a facilitação da transferência de dados entre organizações e a definição de políticas rigorosas de privacidade.

Com a legislação, os cidadãos europeus são beneficiados em questões como: o controle de seus dados, formalização de seus direitos, reformulação da forma com que as organizações tratam os dados dos cidadãos e garante uma circulação segura de dados pessoais na União Europeia (UE) [Almeida Teixeira et al. 2019]. Desde a sua aplicação, o regulamento europeu ganhou protagonismo e serviu de base para o desenvolvimento da LGPD brasileira.

Apesar das exigências complexas, o RGPD não fornece diretrizes específicas quanto à sua implementação, não sendo prescritivo quais tecnologias e metodologias devem ser usadas para alcançar a adequação completa com a lei. Com esse obstáculo, as organizações, em geral, possuem dificuldades em entender o regulamento e em como implementá-lo, em especial empresas com poucos recursos ou com grandes quantidades de dados pessoais. O não cumprimento das disposições do regulamento europeu pode impor multas pesadas às organizações [GDPR 2016].

2.5. LGPD

A LGPD foi criada para aplicar a proteção de dados pessoais em todas as organizações públicas ou privadas, que desempenham qualquer tipo de manipulação sobre os dados dos cidadãos, independente do meio de tratamento. A lei foi baseada no RGPD europeu para evoluir o nível de privacidade, em qualquer operação de coleta, transferência e tratamento de dados pessoais no território nacional [Paini and Zilles 2021]. A lei caracteriza como primordial uma boa comunicação e disponibilização de informações para os usuários e titulares de dados (proprietários dos dados pessoais) sobre a coleta, utilização e tempo de posse dos dados pessoais processados [ROCHA et al. 2019].

A LGPD tem sua aplicação unificada para empresas de qualquer porte, portanto, torna-se necessário o ímpeto em aplicar segurança tecnológica para evitar violações às disposições legais do regulamento [Hussain et al. 2020]. Além disso, faz-se crucial entender as disposições da nova norma e seus impactos práticos. Como exemplos de novas disposições de conformidade podemos citar: a necessidade da criação de relatórios e análises de impactos e riscos à privacidade, receber requisições de clientes para prestação de contas sobre as políticas de privacidade acordadas, e até, a divulgação de incidentes na segurança dos dados.

É notável como a conformidade com a LGPD impõe desafios às empresas e aos gestores públicos. Para alcançar o objetivo de cumprir os requisitos da lei, é essencial a busca por apoio jurídico para estabelecer ou atualizar regimentos internos. Outro aspecto associado aos desafios é a atualização das políticas de SI com abordagens mais amigáveis à privacidade de dados.

A Autoridade Nacional de Proteção de Dados (ANPD) faz parte da estrutura definida pela lei, representando o órgão fiscalizador para o cumprimento da LGPD, além da fiscalização, a ANPD é a responsável por aplicar multas e sanções para empresas que cometem infrações. A depender do grau da contravenção, as sanções podem ser executadas a partir de uma simples advertência, até multas de 2% do faturamento do último exercício de

uma organização, com o limite de até R$ 50 milhões [Lopes and Amaral 2022]. As multas e sanções impostas pela LGPD são fontes de muita preocupação para as organizações, implicando em mudanças e esforços específicos na governança corporativa e governança de dados.

3. Trabalhos Relacionados

A literatura apresenta alguns trabalhos que realizam a avaliação de conjunturas, panoramas, ferramentas, técnicas ou fatores capazes de promover privacidade e cumprir os requisitos das leis de privacidade de dados. Os trabalhos citados são estudos primários e secundários realizados tanto no Brasil como no exterior para entender quais são as múltiplas condutas e necessidades para atender aos requisitos da LGPD e RGPD.

O estudo proposto por Ferreira e Okano, tem o objetivo de verificar o panorama de adequação das organizações brasileiras à LGPD, detectando a opinião de profissionais sobre a lei e as ferramentas, ou métodos capazes de auxiliá-los na implantação. A pesquisa foi executada durante a pandemia do Covid-19 e foi realizada por meio de uma *survey* com 216 profissionais de segmentos variados do mercado. Todas as regiões do Brasil foram contempladas na pesquisa e a análise da pesquisa evidenciou que muitas empresas brasileiras estão iniciando seus projetos de adequação, encontrando desafios complexos, principalmente quanto à sua cultura interna [Ferreira and Okano 2021].

Piurcosky et al. procuram descrever a realidade das implementações das organizações brasileiras quanto à adequação à LGPD [Piurcosky et al. 2019]. A abordagem foi definida para estabelecer como as organizações do sul de Minas Gerais estão se adequando à nova lei. A metodologia foi qualitativa e com raciocínio indutivo, objetivando compreender a realidade das empresas estudadas, coletando dados através de análise de casos múltiplos e entrevistas. O estudo evidenciou que o estado de adequação das empresas ainda é deficitário em atender aos marcos regulatórios da LGPD e foi clarificada a necessidade de modificações consideráveis em processos internos de coleta e armazenamento de dados, assim como, alterações na SI. Além disso, a escassez de recursos tecnológicos e a falta de domínio em boas práticas de SI são fatores limitadores para atender a legislação.

A pesquisa de Teixeira et al. buscou identificar os fatores críticos de sucesso para a implementação do RGPD, que podem facilitar a realização de projetos e são fundamentais para o sucesso das adequações necessárias para a proteção de dados. A metodologia utilizada foi uma revisão sistemática que explorou 32 documentos para responder às questões propostas pela pesquisa [Teixeira et al. 2019]. Como resultado, além dos fatores críticos identificados, o estudo propôs identificar as barreiras e facilitadores da implementação, assim como, descrever os benefícios em cumprir o regimento europeu. Ao todo, 8 fatores críticos foram listados para uma adequação bem sucedida ao RGPD.

No ano de 2021 Silva realizou uma pesquisa com o objetivo de analisar os avanços derivados dos impactos da LGPD na gestão das políticas públicas de dados. A análise inspecionou atividades de municípios brasileiros, e especialmente tomou como estudo de caso a cidade de Belo Horizonte/MG. A principal observação apanhada foi a visualização das mudanças na estruturação da política de governança, para isso, a pesquisa coletou documentos em portais eletrônicos públicos dos municípios e prefeituras analisadas. A principal mudança identificada com a LGPD foi a ampliação de papéis e entidades direciona-

das nos processos decisórios sobre as políticas públicas de dados pessoais [Silva 2021].

O trabalho proposto por Ferrão et al. realizou o diagnóstico de organizações públicas e privadas no Brasil para verificar as condutas de processamento de dados e a adequação com a LGPD, a fim de permitir a percepção geral do panorama de implementação da lei, sobretudo na visão dos profissionais de TI. Coletando a opinião de 105 profissionais de TI, sobre 41 questões tratando do processamento de dados, os resultados colhidos revelam pontos de atenção para LGPD, entre eles o nível baixo de engajamento dos profissionais em tratar de dados pessoais, seguindo as diretrizes especificadas na organização. Outro ponto relevante é o desconhecimento de artefatos considerados eficientes e amigáveis à privacidade, seguindo os princípios da legislação [Ferrão et al. 2021].

Embora os autores apresentem lições aprendidas e até implementações concretas com a aplicação de vários processos, não há estudos que compilam múltiplas soluções organizacionais para garantir a privacidade. É possível verificar limitações nos trabalhos citados, principalmente em como as soluções podem ser conectadas para promover avanços na gestão de dados, mudanças na cultura organizacional e processos de negócio. Neste contexto, este trabalho se destaca por implantar uma revisão de soluções organizacionais e a produção de análises e recomendações a partir dos artefatos estudados.

4. Metodologia

Esta pesquisa foi conduzida por meio de uma Revisão Sistemática (RS), um método de estudo que busca dar coerência e sentido a uma investigação específica [Canto et al.]. Para isso, foi formalizado um protocolo de pesquisa que envolve a seleção criteriosa dos estudos relevantes, a definição de critérios formais para o desenvolvimento do trabalho e a descrição detalhada da estratégia adotada para abordar as questões principais propostas.

A RS é constituída diante das seguintes fases: (i) planejamento da RS (definição do protocolo da pesquisa descrevendo as questões de pesquisa, critérios de inclusão e critérios de qualidade); (ii) execução da RS (análise e seleção de estudos); e (iii) resultados da RS. Nesta seção são detalhados os passos seguidos nas fases (i) e (ii). Os resultados e análises referentes à terceira fase são apresentados nas seções 5 e 6.

4.1. Questões de Pesquisa

Com o intuito de identificar e apresentar implementações de metodologias, práticas e processos organizacionais voltados à adaptação e conformidade com os requisitos da legislação nacional, bem como analisar os artefatos apresentados e compreender sua aplicabilidade às demandas da LGPD, as seguintes questões de pesquisa foram adotadas:

- **(Q1)**: Quais são os impactos da LGPD nos processos organizacionais?
- **(Q2)**: Quais são as soluções e artefatos descritos na literatura capazes de solucionar problemáticas de privacidade de dados?
- **(Q3)**: Como as soluções podem ser conectadas para promover avanços na gestão de dados, mudanças na cultura organizacional e processos de negócio?

Além disso, a pesquisa abrangeu tanto as soluções desenvolvidas no Brasil para atender à LGPD quanto os estudos relevantes que impactam o RGPD no período de 2018 a 2023. A análise desses estudos internacionais se mostra relevante devido à alta correlação entre as legislações em termos de requisitos técnicos.

4.2. Critérios de Inclusão

Em relação aos critérios de inclusão, foram considerados estudos disponíveis na íntegra online e redigidos em Português ou Inglês, sem restrição quanto ao número de páginas e de livre acesso. A execução da coleta dos estudos foi no período de dezembro de 2022 a abril de 2023, tendo como referência os portais: Periódicos CAPES, ResearchGate e Mendeley. As categorias dos estudos selecionados compreendem artigos primários, artigos de conferência, artigos de revistas e monografias.

Para seleção de estudos, foi definida uma string de busca com termos relacionados a lei de privacidade de dados brasileira e ao RGPD como também aos objetivos gerais da pesquisa:

1. String para estudos sobre a LGPD: (“LGPD” AND (“implementação” OR “adequação” OR “Segurança da Informação” OR “Governança de Dados” OR “Data Managment” OR “ISO”));
2. String para estudos sobre o RGPD:(“GDPR” AND (“implementation” OR “compliance” OR “ISO” OR “Data Managment”, OR “Information Security”)).

4.3. Avaliacão da Qualidade

Além dos critérios de inclusão foi essencial os itens de qualidade necessários para os estudos. A avaliação de qualidade consistiu em uma análise prévia do conjunto de artigos resultantes após a execução da aplicação dos critérios de inclusão em função dos seguintes pontos:

- **(AQ1)**: O estudo compreende os critérios metodológicos estabelecidos como: Localização (estudos que abordam LGPD e RGPD), Temporal (2018 a 2023) e de Conteúdo (impactos da soluções de adequação à LGPD)?
- **(AQ2)**: O estudo possui uma boa base de conceituação literária em termos de direitos pessoais, privacidade de dados e Segurança da Informação (SI)?
- **(AQ3)**: O estudo contempla informações relevantes de uma implementação concreta dos regulamentos (LGPD E RGPD)?
- **(AQ4)**: O estudo apresenta dados quantitativos e qualitativos relevantes e bem estruturados sobre o artefato abordado?
- **(AQ5)**: O estudo possui uma conclusão satisfatória sobre os impactos da implementação?

A análise dos estudos seguiu os passos:

1. Leitura e análise dos artigos;
2. Para cada artigo lido se considerou os critérios de qualidade descritos de (AQ1) a (AQ5);
3. A avaliação dos estudos foi feita utilizando a escala Likert de 1 a 5, onde 1 indica a pior avaliação do conteúdo e 5, a melhor. A pontuação foi produzida atribuindo pontos para cada critério de qualidade.
4. As pontuações foram consideradas como o fator de referência de qualidade para aceitação do estudo.

4.4. Estudos selecionados e apresentação dos resultados

Com a aplicação da busca utilizando as strings e os engenhos de buscas definidos, obteve-se 82 artigos resultantes. Após análise dos critérios de inclusão ficamos com uma amostra de 51 trabalhos. A partir deste resultado aplicamos a avaliação dos parâmetros de qualidade, resultando em 17 estudos conforme especificado na Tabela 1. Esses estudos foram divididos em seis áreas-chave relacionados aos impactos das soluções propostas para a adequação à LGPD. Os trabalhos selecionados e as avaliações de qualidade são identificados na Tabela 1.

Tabela 1. Estudos selecionados e sua avaliação de qualidade

Estudo	Referências	AQ1	AQ2	AQ3	AQ4	AQ5	Nota
E1	Metodologia Scrum: Uma aliada na implementação da LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E2	The critical success factors of GDPR implementation: a systematic literature review	1,0	1,0	1,0	1,0	0,5	4,5
E3	Segurança da informação e da transparência e a proteção de dados na administração pública: lgpd, acesso à informação e os incentivos à inovação e à pesquisa científica e tecnológica no âmbito do estado de minas gerais	1,0	1,0	0,5	0,5	0,5	3,5
E4	Prestação dos serviços públicos à luz da lei geral de proteção de dados (lgpd) – a case study	1,0	1,0	0,5	0,0	0,5	3,0
E5	Segurança da informação: A ISO 27.001 como ferramenta de controle para LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E6	O mapeamento do modelo data management maturity (dmm) a lei geral de proteção de dados (lgpd)	1,0	1,0	1,0	1,0	1,0	5,0
E7	Framework para identificar o nível de conformidade dasempresas brasileiras do setor químico no processo deadequação à lei geral de proteção de dados pessoais	1,0	1,0	1,0	1,0	1,0	5,0
E8	Análise da implantação da gestão de riscos na tecnologia da informação: um estudo de caso	1,0	1,0	1,0	1,0	1,0	5,0
E9	O impacto da lgpd no desenho da política de governança de dados nos municípios: o caso de belo horizonte/mg	1,0	1,0	0,5	0,0	0,5	3,0
E10	LGPD análise dos impactos da implementação em ambientes corporativos: estudo de caso	1,0	1,0	0,5	0,5	1,0	4,0
E11	From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls.	1,0	1,0	1,0	1,0	1,0	5,0
E12	A GDPR-compliant Risk Management Approach based on Threat Modelling and ISO 27005	1,0	1,0	1,0	1,0	1,0	5,0
E13	Achieving GDPR compliance of BPMN process models	1,0	1,0	1,0	1,0	1,0	5,0
E14	Lgpd o novo desafio para as organizações: Exemplos de frameworks para diagnosticar este novo cenário.	1,0	1,0	1,0	1,0	1,0	5,0
E15	Análise de conformidade de processos de negócios em relação a LGPD	1,0	1,0	1,0	1,0	1,0	5,0
E16	Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução	1,0	1,0	1,0	1,0	1,0	5,0
E17	Diagnostic of data processing by Brazilian organizations—a low compliance issue	1,0	1,0	0,5	0,5	0,5	3,5

Em termos de apresentação e síntese, este estudo adotou uma revisão sistemática narrativa para sintetizar os resultados de estudos qualitativos, quantitativos e mistos, transformando suas descobertas em achados qualitativos. Essa abordagem permite uma análise descritiva e indutiva, capacitando a reinterpretação e conexão de diferentes estudos para gerar novas conclusões sobre o tema.

5. Análise dos Resultados

Dos estudos selecionados na RS, emerge um panorama abrangente de implicações em empresas e organizações durante o processo de adequação à LGPD. Observou-se, por exemplo, que o desenvolvimento das ações necessárias para a conformidade com a LGPD é um projeto que exige uma mudança na cultura empresarial e na atualização e implementação de processos organizacionais, sobretudo na cultura da gestão e governança das informações pessoais. Tais mudanças envolvem investimentos em recursos tecnológicos, operacionais e humanos, por meio de ações planejadas e relacionadas, para assim, criar uma estratégia capaz de sensibilizar as ações sobre o tratamento de dados [Montolli 2020][Rodrigues and de Paula 2022][de Melo Filho et al. 2023].

No contexto empresarial, o uso massivo da TI, para evoluir na perspectiva estratégica da proteção dos ativos de informação das organizações. As empresas devem oferecer um conjunto de normas e diretrizes formalizadas capazes de promover segurança em seus sistemas de segurança da informação e nos seus processos internos, que promovem a transferência de dados [ROCHA et al. 2019]. Tais diretrizes e normas formam a governança de dados que ocorre por meio da institucionalização de regras, que promovem as ações dos indivíduos associados aos processos organizacionais [Silva 2021].

Diante das novas demandas direcionadas às organizações, com muitos ativos de informações e muitas operações sobre dados, um dos principais obstáculos enfrentados está no fato de que as transformações culturais e adaptações às regras das novas legislações de proteção de dados pessoais não são de fácil execução e geralmente não são aplicadas rapidamente como desejado [Lima 2020]. As legislações demandam o alto custo e investimento para muitas empresas e órgãos públicos em:

- Estrutura humana e operacional;
- Contratação de novos profissionais (também existe investimento em certificações, treinamentos);
- Aquisição de equipamentos;
- Estimulo conjunto entre todas as áreas da organização para promover a mudança cultural.

As demandas coletivas para desenvolver processos organizacionais de adequação à LGPD é um ponto essencial para gerar uma cultura de proteção de dados, que ainda não foi consolidada [Lugati and de Almeida 2022]. Logo um período de adaptação coletiva se faz necessário, visando compreender os objetivos das novas disposições sobre proteção de dados, e em adição, entender como as mudanças são aplicadas.

Algumas estratégias para uma disseminação coletiva eficiente é a criação de cartilhas, elaboração de informes, produção de instruções rápidas e capacitação direcionada, como estabelecido nos estudos [ROCHA et al. 2019][de Melo Filho et al. 2023].

Ao estudar a implementação de uma legislação, como a LGPD em uma empresa, é importante verificar as mudanças em seus processos administrativos e de negócio, para analisar os aspectos mais diversos da organização, observando quais as maiores dificuldades encontradas e como cada membro ou divisão organizacional deve se adaptar ao processo de implementação [Lugati and de Almeida 2022].

Visto que algumas dificuldades da adequação à LGPD estão em problemas como: estabelecimento de políticas formais, gestão de dados, auditorias, mapeamento de da-

dos e mapeamento de fluxo de dados por parte das organizações, torna-se evidente que, alguns métodos, modelos e padrões podem ser de utilidade vital para auxiliar a conformidade com LGPD. Nas seções seguintes, são apresentadas algumas das soluções aplicadas durante o processo de adequação à LGPD identificadas nos estudos analisados nesta pesquisa. Essas soluções foram classificadas em 4 categorias: *frameworks*; modelo de gestão de dados; referência a padrões; e, modelagem de negócios.

5.1. *Frameworks*

Um *framework* é um conjunto de ferramentas, práticas e bibliotecas que servem como base para o desenvolvimento de algo específico, como um software, um sistema ou até mesmo processos organizacionais. Sua principal missão é agilizar o desenvolvimento, ao mesmo tempo em que promove, frequentemente, maior qualidade nos resultados finais. Isso acontece porque um *framework* opera com uma estrutura de desenvolvimento bem estabelecida e validada. Dentro desse contexto, foram identificados diversos *frameworks* que podem auxiliar as organizações na sua jornada de conformidade com a LGPD. Um exemplo desse tipo de abordagem é o LGPD Model Canvas [Okano et al. 2021].

O LGPD Model Canvas é uma ferramenta visual inspirada na legislação de proteção de dados, que também incorpora princípios ágeis e a ideia de "privacidade desde a concepção" proposta pelo RGPD. Esse modelo visual prioriza a proteção de dados nos aspectos organizacionais, sugerindo que a atenção aos dados pessoais deve estar presente desde o início de qualquer projeto e na concepção de todos os processos.

Essa ferramenta é dividida em duas etapas distintas. A primeira envolve a avaliação dos processos que lidam com dados pessoais no momento atual da organização, registrando como a proteção de dados está sendo implementada. A segunda etapa é voltada para um mapeamento futuro, alinhando os objetivos empresariais com as lacunas e oportunidades identificadas na etapa anterior [Okano et al. 2021].

Para implementar o LGPD Model Canvas, a organização deve promover sessões de *brainstorming*, permitindo que grupos multidisciplinares gerem ideias diversas. Essa atividade busca influenciar a cultura organizacional, tornando-a centrada na inclusão da privacidade como elemento fundamental dos processos. Isso amplia a discussão sobre os objetivos principais da empresa e o valor das disposições da LGPD para a organização. O *framework* é composto por nove blocos, incentivando uma abordagem colaborativa e definindo formalmente diretrizes para o preenchimento descritivo (Figura 1).

O preenchimento do LGPD Model Canvas é realizado para cada processo, alinhando os principais produtos/serviços oferecidos pela empresa, seus papéis como controlador/operador, bem como as entidades envolvidas (internas e externas) e a complexidade dos processos que lidam com dados pessoais [Okano et al. 2021].

Outro *framework* identificado na RS é o FRAMEWORK LGPD [Silva et al. 2021], uma construção baseada em referências e soluções de várias legislações internacionais, como RGPD, *California Consumer Privacy Act* e LGPD, buscando integrar atividades organizacionais para solucionar inadequações com a lei brasileira.

O FRAMEWORK LGPD foi desenvolvido para validar o nível de conformidade e orientar as empresas na adaptação à LGPD, delineando um conjunto de etapas e tarefas

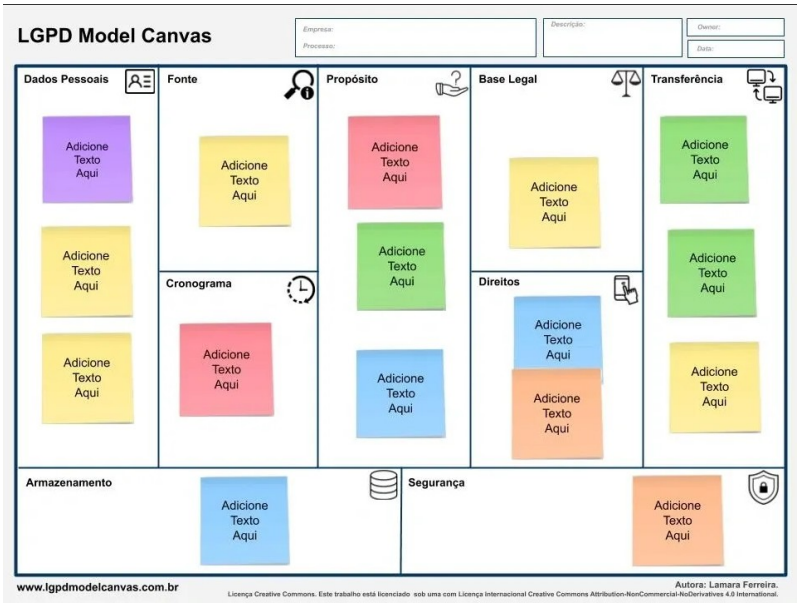

Figura 1. LGPD MODEL CANVAS. Fonte: [Okano et al. 2021]

a serem executadas, seguindo uma estrutura similar aos modelos de avaliação de qualidade de software. Este *framework* compreende as fases de iniciação, reconhecimento, validação, desenvolvimento e encerramento.

Ambos os *frameworks* possuem como principal característica a avaliação dos processos e a verificação da conformidade com a LGPD. Embora utilizem instrumentos semelhantes, como o *brainstorming* para análise e coleta de detalhes dos processos internos, suas abordagens e produtos gerados são distintos. O LGPD Canvas Model destaca-se pelo aspecto visual, enquanto o FRAMEWORK LGPD não especifica muitas ferramentas além da modelagem de fluxo de dados e da produção de documentação formalizada [Silva et al. 2021].

A aplicação desses métodos facilita as operações com dados pessoais, proporcionando uma visão abrangente sobre o tratamento de dados. Isso favorece a análise empresarial, tornando-a mais estruturada, ampliando a compreensão sobre a LGPD e envolvendo diversos setores e departamentos. No entanto, a principal limitação desses *frameworks* é sua aplicabilidade às Tecnologias da Informação e Comunicação (TIC). Nesse sentido, é fundamental realizar testes e estudos de caso para associar esses artefatos aos sistemas utilizados pelas empresas [Okano et al. 2021].

5.2. Modelo de Gestão de Dados

No âmbito da gestão e modelos de dados, destacamos no estudo de [Marques 2020], o modelo *Data Management Maturity* (DMM) do Instituto *Capability Maturity Model Integration*. O DMM é concebido como um modelo de referência abrangente para o aprimoramento de processos, visando apoiar organizações a alcançar progressivamente um nível avançado de maturidade no gerenciamento de dados.

Este modelo busca representar o estado atual da empresa em relação aos seus dados, estabelecendo um conjunto de boas práticas para fortalecer a governança das informações institucionais. Desta forma, auxilia as organizações na avaliação de suas

capacidades, identificação de pontos fortes e lacunas, e na alavancagem de seus ativos de dados para melhorar o desempenho dos negócios. A grande razão para a interconexão desse modelo com os requisitos de proteção de dados é o fato de que modelos de administração, especialmente modelos completos como o DMM, têm se tornado relevantes por promover velocidade, robustez e eficiência operacional no desenvolvimento de sistemas seguros e processos que operam sobre dados [(CMMI) 2019].

A LGPD demanda medidas para a proteção de dados pessoais, aprimoramento da rastreabilidade dos dados e promoção de prestação de contas com titulares e entidades como a ANPD. Nesse contexto, algumas características do DMM revelam um potencial otimista para sua aplicação na conformidade com a lei brasileira, uma vez que sua principal função do DMM é centralizar a gestão de dados e integrar os sistemas e processos ao modelo, proporcionando eficiência na precisão de dados [Marques 2020].

A maturidade do gerenciamento de dados, objetivo explícito do modelo, é determinada pela capacidade da organização em aplicar o DMM para controlar e gerir eficientemente seus dados de forma estratégica e planejada. A estrutura do modelo compreende duas partes principais: categorias e áreas de processos (Figura 2).

CATEGORIAS	ÁREAS DE PROCESSO
Estratégia de Gestão de Dados	Estratégia de Gestão de Dados
	Comunicação
	Função de Gestão de Dados
	Caso de Negócio
	Financiamento do Programa
Governança de Dados	Gestão de Governança
	Glossário de Negócios
	Gestão de Metadados
Qualidade de Dados	Estratégia de Qualidade de Dados
	Perfil de Dados
	Avaliação da Qualidade dos Dados
	Limpeza de Dados
Operações de Dados	Definição dos Requsitos dos Dados
	Gestão de ciclo de vida dos dados
	Gestão de Provedor
Plataforma e Arquitetura	Abordagem Arquitural
	Padrões Arquiteturais
	Plataforma de Gestão de Dados
	Integração de Dados
	Dados Históricos, Arquivamento e Retenção
Processos de Suporte	Medição e Análise
	Gerência de Processos
	Garantia de Qualidade de Processos
	Gestão de Risco
	Gestão de Configuração

Figura 2. Categorias e Áreas de Processos DMM. Fonte: Adaptado de [(CMMI) 2019].

Outro componente essencial do DMM são as capacidades dos processos, que especificam um nível de maturidade para definir o quão efetivo é o gerenciamento de dados e como cada processo foi aprimorado por diferentes práticas. Os cinco níveis de capacidade são: Executado, Gerido, Definido, Medido e Otimizado [(CMMI) 2019]:

A pesquisa de [Marques 2020] destaca medidas do DMM que podem apoiar na promoção de conformidade com a LGPD. A ferramenta contribui significativamente ao

proporcionar a visibilidade dos dados, incluindo fontes e fluxos das informações dos titulares na organização. Dado que a LGPD exige uma governança de dados focada nos direitos dos titulares, o DMM emerge como uma solução para muitos desafios relacionados ao tratamento de dados. O modelo assegura uma gestão clara sobre como os dados pessoais são coletados, onde e por quanto tempo serão arquivados, e quais os processos e procedimentos podem encerrar o tratamento de dados, de maneira transparente e ética.

Outra funcionalidade relevante é encontrada no mapeamento dos dados organizacionais, possibilitando rastreabilidade interna na organização. Essa atividade melhora o controle de quais funcionários, setores ou sistemas realizaram operações de dados e quais detêm a posse ou acesso aos dados, elevando assim o nível de proteção de dados e de segurança da informação.

Além disso, [Marques 2020] também define que a rastreabilidade é capaz de definir quais processos internos são afetados pelos dados e quais procedimentos possuem prioridade, avaliando sempre a complexidade e criticidade na operação de dados. Contudo, falta uma análise mais aprofundada quanto a aplicação da DMM atende aos requisitos da LGPD. Adicionalmente, é fundamental compreender como a modificação dos processos organizacionais pode se alinhar com outras modelagens e normas de segurança de SI como a série ISO 27000.

5.3. Padrões de Referência

Uma das diretrizes mais relevantes da LGPD, e de muitas legislações que resguardam dados pessoais, é o desenvolvimento de medidas de segurança, sejam técnicas ou administrativas para proteção de dados. Para isso, muitas organizações optam por realizar a adoção de padrões de segurança reconhecidos internacionalmente e construídos por instituições renomadas no ramo de normas e padrões. A ISO 27001 é uma das normas mais referenciadas no meio organizacional para realizar a segurança da informação, concedendo práticas robustas para resguardar e proteger dados corporativos (incluindo dados pessoais) [Almeida Teixeira et al. 2019].

Os Artigos 49 e 50 da LGPD são os artigos que citam diretamente a obrigação das instituições na utilização de padrões eficientes, na promoção de segurança dos dados. Nesse contexto, a ISO 27001 é qualificada para aprimorar requisitos gerais para implementar, monitorar e melhorar a administração organizacional nos aspectos de segurança dos dados, além de possuir ferramentas para mitigação de risco, fatores interessantes para cumprir uma lei de privacidade de dados [Lima 2020]. Para adotar a norma, um dos primeiros passos de execução das empresas é a criação de uma política regulamentadora das práticas em SI [Piurcosky et al. 2019].

A Política de Segurança da Informação (PSI), é uma documentação que determina técnicas e procedimentos sobre o fluxo de informação interno e externo e quais entidades ou sistemas processam e transferem tais informações. Os princípios da PSI precisam ser minuciosos e disseminados a todos os colaboradores da segurança das informações empresariais [ROCHA et al. 2019].

A ISO 27001 propõe instruções globais contendo subdivisão em onze seções que abordam procedimentos desde gestão de ativos e segurança em recursos humanos. O objetivo final da norma ISO 27001 é utilizar as políticas do PSI, em conjunto com planos de tratamento de risco e auditorias internas para desenvolver o Sistema de Gestão

de Segurança da Informação (SGSI). O SGSI é o sistema (não necessariamente automatizado) capaz de incluir toda abordagem organizacional nas ações para assegurar a proteção das informações empresariais, seguindo os principais princípios da SI. A pesquisa de [ROCHA et al. 2019], a norma também está diretamente relacionada com os principais requisitos da LGPD.

O tempo para a preparação da certificação ISO/27001 é variável, pois requer a implementação e adoção de todos os requisitos, políticas, procedimentos, e controles requeridos para todos os âmbitos da organização. O *roadmap* típico de implementação de um SGSI é especificado pelo próprio ISO [ISO/IEC 2019].

Outros padrões da série 27000 podem ser utilizados em conjunto para elaborar o SGSI, a ISO 27002 pode ser aliada a norma anterior adicionando mais controles e boas práticas que podem ser usados como guias para uma gestão de risco [Diamantopoulou et al. 2020]. Já o estudo de [Flores and Perugachi 2023] explica a possibilidade do desenvolvimento de modelagem de ameaças para gerenciamento de riscos, usando a ISO 27005 como base para integrar os controles de segurança da ISO 27001/27002. A modelagem implementa um catálogo inicial de ameaças que possibilita um tratamento de risco mais eficiente.

A pesquisa de [ROCHA et al. 2019] elaborou uma comparação entre as disposições da LGPD e da ISO 27001, para determinar diretrizes capacitadas a ajudar as empresas a cumprir os requisitos da legislação. O resultado observou que a lei brasileira possui uma correspondência direta e pode utilizar 67,86% dos itens obrigatórios da norma. Os 32% de não correspondência se referem à documentação mínima requerida pelo ISO, o que não significa que as práticas do padrão são conflituosas com a conformidade da LGPD.

5.4. Modelagem de Negócio

Os processos de negócio de uma organização são as atividades que especificam a execução das obrigações dos funcionários e como toda a sequência lógica de tarefas deve ser executada. Nessa direção, a modelagem dos processos de negócio propõe artefatos que simbolizam os processos da empresa e podem ser utilizados para modelar os procedimentos que envolvem questões de privacidade e requisitos da LGPD [Menegazzi 2021].

O estudo abordado por [Agostinelli et al. 2019] constata que muitas das modelagens de processos de negócio são adequadas para expressar a colaboração entre partes interessadas e em compreender fluxos de dados, no entanto, pouco foi avançado para modelar processos, a fim de evitar violações de dados ou de privacidade. Diante desta demanda, o estudo defende que a proteção de dados dos cidadãos deve ser protagonista nos modelos de negócio e deve ser introduzida a partir do design dos processos e não como uma ação corretiva. O estudo propõe a modelagem das principais restrições de privacidade delineadas no RGPD europeu, restrições essas que também são aplicáveis à LGPD.

Tomando como exemplo a aplicação de modelagem BPMN, focadas no RGPD para uma companhia telefônica, são apresentados sete padrões de privacidade modelados sem que nenhum símbolo BPMN adicional fosse necessário. Os sete padrões desenvolvidos foram: Violação de dados, Consentimento, Direito de Portabilidade, Direito de

Acesso, Direito da finalização do Tratamento, Direito de Correção de Dados e Direito de Esquecimento [Agostinelli et al. 2019].

De maneira análoga, o estudo [da Costa Júnior 2020] se dedica à conformidade dos processos de negócio diante das exigências da Lei Geral de Proteção de Dados, apresentando um método de modelagem de processos utilizando a notação BPMN. Denominado LGPD4BP (LGPD for Business Process), o método proposto neste trabalho consiste em um questionário de avaliação da conformidade dos processos em relação à LGPD, um Catálogo de Padrões de Modelagem e um Método de Modelagem de processos alinhados com as diretrizes da LGPD.

O catálogo de padrões e modelagens foi criado para modelar requisitos específicos da lei. No catálogo, foram modelados 9 padrões: Consentimento, Direito de Acesso, Transferência internacional de dados, Portabilidade, Vazamento de Dados, Revisão de tomada de decisão automatizada, Retificação de Dados, Direito de Eliminação ou Esquecimento, Confirmação da existência de tratamento e direito de acesso.

Já o método de modelagem, é apresentado como um processo em BPMN, criado para orientar o modelador de negócio em modelar um processo, ou corrigir algum modelo não compatível com a LGPD. Tanto o Catálogo de Padrões de Modelagem, como o Método de Modelagens, estão disponíveis em um portal disponibilizado pelo autor [1]. Para testar a modelagem em um exemplo concreto, o método LGPD4BP foi utilizado em uma instituição de ensino (escola de ensino fundamental e médio).

Com isso, em seu trabalho [da Costa Júnior 2020] avalia que o LGPD4BP pode ser usado como uma referência para modelar processos de negócios em conformidade com a LGPD, no entanto, é necessário apontar que a metodologia ainda é manual e não automatizado, dependendo do conhecimento dos projetistas, pois o BPMN não pode ser considerada uma linguagem acessível para qualquer profissional. Outro aspecto importante é a necessidade de validar a integralidade do LGPD4BP com especialistas em privacidade.

Ao incorporar as modelagem BPMN com elementos de proteção de dados, as pesquisas conduzidas por [Agostinelli et al. 2019] e [da Costa Júnior 2020] enriquecem a capacidade de modelagem de negócios com diretrizes específicas para o tratamento de informações pessoais. Dessa forma, os processos de negócio emergem como pilares fundamentais para a segurança no manejo adequado de dados. Além disso, as modelagens de negócio possibilitam o estabelecimento ágil e eficaz de medidas organizacionais para lidar com questões relacionadas à manipulação de dados.

6. Recomendações

Esta seção resume, em termos de recomendações, a análise da revisão sistemática, destacando seu potencial para proporcionar resultados concretos na busca pela conformidade com a LGPD. A análise aborda artefatos associados aos processos organizacionais de adequação à legislação brasileira, bem como soluções tecnológicas voltadas para a SI.

O início da implementação da adequação à LGPD requer, acima de tudo, a participação de profissionais e gestores da organização. Antes da adoção de qualquer

[1] catálogo e métodos de negócio disponível em: https://sites.google.com/view/lgpd4bp

método, ferramenta metodológica ou tecnológica, é essencial incluir esses *stakeholders* para especificar os objetivos e metas desejados no novo contexto imposto pela legislação. Posteriormente, é necessário o envolvimento de atores internos para aprimorar as manipulações de informações e criar uma cultura organizacional motivada a cumprir os requisitos da LGPD.

A partir da atribuição de papéis, grupos e profissionais focados na conformidade da LGPD, é possível iniciar as mudanças internas, especialmente nos processos organizacionais que influenciam na operação de dados e na tomada de decisão dos procedimentos de negócio executados.

Muitos dos artefatos coletados na revisão sistemática evidenciam que qualquer metodologia adotada para que um órgão se adeque às cláusulas estipuladas pela LGPD, deve promover o alinhamento de objetivos e incluir a privacidade de dados pessoais em processos vitais da empresa. Em muitos casos, torna-se necessário descrever ou modelar os processos atuais para atualizá-los e utilizá-los diante das novas metas estabelecidas. A modelagem dos processos é uma ferramenta poderosa para institucionalizar a execução de tarefas de adequação à proteção de dados.

Além do mapeamento dos processos, muitos dos artefatos apresentados na revisão estimulam a produção de documentação que detalha o mapeamento de dados e o fluxo de dados, além do mapeamento de riscos e inconformidades. A documentação e artefatos produzidos podem fornecer informações relevantes para a produção de registros obrigatórios pela ANPD, como o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

As soluções mais complexas, relacionadas aos processos de adequação organizacionais, demandam a produção de um controle total dos dados pessoais em grandes organizações ou conglomerados, que possuem inúmeros recursos, procedimentos e sistemas. Neste caso, as soluções estabelecidas buscam formalizar uma Política de Segurança da informação, que define regras administrativas para tratar da proteção de dados.

Para organizações que possuem recursos técnicos e profissionais e lidam com muitos processos sensíveis às demandas da LGPD, é possível prospectar a adoção de normas de segurança para transformar a PSI. Isso, em conjunto com planos de tratamento de risco e auditorias internas, pode resultar no desenvolvimento do Sistema de Gestão de Segurança da Informação. O desenvolvimento do SGSI é um processo complexo que pode requer das empresas a utilização de modelos complexos para compreender toda a estrutura operacional, estabelecer padrões de comunicação e planejamento.

Após a análise obtida sobre as soluções relacionadas aos processos organizacionais de adequação, este trabalho propõe um conjunto de recomendações para adequação à LGPD para qualquer organização que trata dados pessoais (entidades do poder público ou privadas), unindo nossas percepções com todo o processo de revisão da literatura e interconexão dos estudos analisados. As recomendações além de propor ações concretas para atender a LGPD também se relacionam com a temática de SI ao propor a melhoria do tratamento dos ativos de informação tanto na perspectiva de privacidade de dados como na segurança dos ativos de informação organizacionais.

1. **R1 - Integração de atores para inicialização da conformidade com a LGPD**
   Descrição: É fundamental integrar diversos atores para fomentar uma cultura or-

ganizacional que promova a privacidade de dados. Essa integração visa não apenas a criação, mas também o desenvolvimento contínuo da cultura, abrangendo a especificação de objetivos, a elaboração do planejamento e a execução de todas as ações necessárias conforme exigido pela legislação. Esses atores englobam profissionais, gestores, auditores internos e externos, além dos agentes de tratamento especificados na LGPD, como controladores e operadores, juntamente com os encarregados de dados.

Soluções envolvidas:

- *Framework* LGPD Model Canvas que envolve setores, funcionários e entidades para atualizar processos internos;
- *Framework* LGPD que especifica a criação de um comitê interdisciplinar de governança de dados;
- ISO 27001 que especifica a necessidade do envolvimento da alta administração nos esforços de conformidade.

Recomendado para: Todas as organizações que demandam engajamento de funcionários, gestores, administradores, agentes de tratamento para as ações de adequação.

2. **R2 - Mapeamento de dados e fluxo de dados**

   Descrição: É vital verificar a natureza dos dados processados e o fluxo de coleta, processamento, análise e compartilhamento de dados.

   Soluções envolvidas:

   - O *Framework* LGPD MODEL CANVAS pode apoiar a descrição dos tipos de dados e seus fluxos, tanto para empresas de médio e de pequeno porte, ou até microempreendedores individual que processam dados pessoais armazenados em um único sistema, ou em documentos físicos;
   - Para organizações de grande porte. ou órgãos públicos com quantidade massiva de dados de cidadãos o DMM apoia os mapeamento, sobretudo nas categorias de processo de qualidade de dados e operação de dados.

   Recomendado para: O processo de mapeamento de dados é essencial para qualquer organização que pretende a adequação com a LGPD.

3. **R3 - Relatório de impacto à proteção de dados pessoais - RIPD**

   Descrição: A construção do RIPD é um processo especificado na LGPD para prestação de contas das organizações com a autoridade nacional ANPD. A documentação deve prover detalhes do estado presente de conformidade, identificando os riscos de violação dos princípios da lei e os procedimentos de salvaguarda. As modelagens de processo e a documentação das ações e recursos alocados para atender à proteção de dados são recursos que facilitam a construção do RIPD.

   Soluções envolvidas:

   - *Framework* LGPD e LGPD MODEL CANVAS para criação de um RIPD inicial ou atualizado com a evolução da conformidade;
   - O modelo DMM é mais viável para apoiar a produção do documento em grandes corporações, visto que, o RIPD precisa gerar detalhes completos sobre aspectos minuciosos de muitos setores e sistemas.

   Recomendado para:

   - Qualquer organização que armazena uma quantidade significante de informações pessoais para receber demandas ou cobranças da autoridade nacional;

- É especialmente necessária para órgãos públicos e empresas com sistemas de informação que processam dados de usuários.

4. **R4 - Modelagem de processos de conformidade à LGPD**
   Descrição: Diagnosticar as exigências estabelecidas pela LGPD nos procedimentos organizacionais, visando modelar processos adaptados à proteção e privacidade de dados, utilizando a notação BPMN, por exemplo. É imperativo que as instituições delineem claramente suas necessidades e modelem os processos essenciais para garantir o cumprimento dos direitos dos titulares de dados, atendendo, assim, às demandas da autoridade nacional.
   Soluções envolvidas:
   - Modelagem de negócio com a notação BPMN;
   - O *framework* LGPD Model Canvas pode ser utilizados para traduzir as modelagens de processos em linguagem natural, para disseminar os procedimentos e possibilitar o treinamento e instrução das atividades.

   Recomendado para: Empresas de médio e grande porte com multiplicidade de processos serem adaptados aos requisitos da LGPD.
5. **R5 - Criação de Política de Segurança da Informação - PSI**
   Descrição: O desenvolvimento da PSI emerge de uma documentação que descreve as regras, delineando procedimentos e ações adotadas para garantir a SI. Essa documentação abrange minuciosamente o fluxo e o ciclo de vida dos dados, incluindo uma lista detalhada de entidades, artefatos e sistemas que processam e compartilham informações. A precisão desse detalhamento é intrinsecamente ligada à Lei Geral de Proteção de Dados, pois ao especificar os pormenores das informações organizacionais, os dados pessoais são correlacionados às exigências específicas de segurança.
   Soluções envolvidas: A incorporação da Norma 27001 delineia os passos iniciais para o desenvolvimento da PSI, contribuindo para a certificação do padrão de segurança.
   Recomendado para:
   - Empresas de médio e grande porte com multiplicidade de processos e regras a serem adaptados aos requisitos da LGPD;
   - Empresas que possuem, desenvolvem e/ou gerenciam sistemas da informação ou são baseadas em produção de tecnologia (sistemas digitais / aplicações para internet).
6. **R6 - Desenvolvimento do Sistema de Gestão de Segurança da Informação - SGSI**
   Descrição: O SGSI é um sistema (não necessariamente um sistema automatizado) que descreve e engloba todos os procedimentos e políticas organizacionais para a SI. A correlação dos requisitos impostos pela LGPD com as diretrizes estabelecidas pela norma ISO 27001, que formaliza a implementação do SGSI, representa uma garantia sólida da pertinência e utilidade desse sistema na proteção efetiva dos dados.
   Soluções envolvidas: O objetivo final da norma ISO 27001 é o desenvolvimento do SGSI. Outros padrões da série ISO 27000 podem ser adotados para implementar um SGSI mais completo e mais robusto para a segurança da informação.
   Recomendado para: Corporações que buscam a certificação de padrões e normas de segurança conceituados.

7. **R7 - Modelo de governança de dados**
   Descrição: As organizações podem utilizar um modelo de governança de dados capaz de analisar, sistematizar e aprimorar a maturidade no gerenciamento de dados. O modelo deve ser capaz de representar o estado atual da organização, em relação a manipulação e gestão de seus dados. Além do seu estado, deve definir práticas que auxiliem na governança das informações e identificar as oportunidades, pontos fortes e lacunas, para assim, possibilitar a melhora no desempenho de governança e execução das atividades de negócio.
   Soluções envolvidas: O DMM para a análise documentação, implementação e melhoramento de processos internos, relacionados à governança e processamento de dados.
   Recomendado para: Corporações ou instituições do serviço público com entidades, departamentos e fluxo de dados complexos. Dotada de profissionais especializados em governança de dados, aptas a realizar capacitação e treinamentos contínuos, e por fim aptas em destinar recursos tecnológicos e humanos para adaptar seus processos.

A Tabela 2 expõe a associação entre os estudos relacionados as recomendações desenvolvidas:

Tabela 2. Associação entre recomendações e estudos relacionados

Recomendação	Referências
R1	E3, E5, E7, E14 e E16
R2	E5, E6, E14 e E17
R3	E1, E7, E9, E14 e E16
R4	E13, E14, E15 e E16
R5	E5
R6	E5, E11 e E12
R7	E2, E6 e E10

Com as recomendações obtidas, conseguimos explorar o principal resultado pretendido em nossa pesquisa, desenvolvendo propostas com o objetivo de testar e melhorar a SI, assim como apresentar estratégias para a aplicação da LGPD em diferentes organizações brasileiras, sejam públicas ou privadas.

7. CONCLUSÕES

Este estudo conduziu uma revisão sistemática com o propósito de reunir técnicas e soluções destinadas a mitigar os riscos à privacidade e atender às demandas da LGPD, proporcionando artefatos que orientam as práticas organizacionais na elaboração de planejamentos e condutas relacionadas a dados pessoais. A revisão evidenciou que a diversidade de estratégias implementadas nos últimos anos, em muitos casos, foi desenvolvida de forma desconexa. Diante desse cenário, as soluções de conformidade com as legislações foram concebidas de maneira paralela, revelando uma lacuna na especificação de todos os recursos e artifícios necessários para uma implementação abrangente da LGPD, alinhada às exigências específicas das organizações.

Também como resultado da RS, o trabalho identificou sete recomendações de implementação, visando executar boas práticas de privacidade e estabelecer processos seguros e alinhados aos requisitos da LGPD na temática de Segurança da Informação e governança de dados. Espera-se que essas recomendações contribuam para a implementação da LGPD de forma consistente e eficiente. Além disso, elas podem ser aplicadas por organizações do Brasil, estaduais ou privadas de todos os portes e setores, independentemente de seu nível de maturidade em privacidade.

As principais limitações deste trabalho residem no processo de coleta de estudos, que se restringiu aos três portais que disponibilizam acesso livre aos artigos, além da restrição aos idiomas português e inglês. Em futuras pesquisas, pretende-se não apenas detalhar as recomendações, mas também aplicá-las em uma organização que detenha dados pessoais, e realizar a integração dos processos organizacionais com técnicas de Tecnologia da Informação para implementar soluções em Sistemas de Informação.

Referências

Agostinelli, S., Maggi, F. M., Marrella, A., and Sapio, F. (2019). Achieving gdpr compliance of bpmn process models. In *Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, June 3–7, 2019, Proceedings 31*, pages 10–22. Springer.

Almeida Teixeira, G., Mira da Silva, M., and Pereira, R. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4):402–418.

Canto, G., Porporatti, A., De Souza, B., Massignan, C., agostines Mir, C., Casett, E., Porfírio, G., et al. Revisões sistemáticas da literatura: guia prático.

(CMMI), T. C. M. M. I. I. (2019). Data management maturity (dmm)sm model. Disponível em `https://stage.cmmiinstitute.com/getattachment/cb35800b-720f-4afe-93bf-86ccefb1fb17/attachment.aspx`. Acesso em: 21 fev 2023.

da Costa Júnior, E. A. (2020). *Análise de conformidade de processos de negócios em relação a LGPD*. PhD thesis, UNIVERSIDADE FEDERAL DE PERNAMBUCO.

Daoudagh, S. and Marchetti, E. (2022). The gdpr compliance and access control systems: Challenges and research opportunities. In *ICISSP*, pages 571–578.

Daryus (2023). Pesquisa nacional 2022-2023 - privacidade e proteção de dados pessoais. Disponível em `https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados`. Acesso em: 5 abril 2023.

de Melo Filho, D. R., de Aguiar Pereira, J. V., Queiroga, T. A. C., and Carr, C. N. (2023). Metodologia scrum: Uma aliada na implementação da lgpd. *Research, Society and Development*, 12(4):e22712441189–e22712441189.

Diamantopoulou, V., Tsohou, A., and Karyda, M. (2020). From iso/iec27001: 2013 and iso/iec27002: 2013 to gdpr compliance controls. *Information & Computer Security*, 28(4):645–662.

Ferrão, S. É. R., Carvalho, A. P., Canedo, E. D., Mota, A. P. B., Costa, P. H. T., and Cerqueira, A. J. (2021). Diagnostic of data processing by brazilian organizations—a low compliance issue. *Information*, 12(4):168.

Ferreira, L. and Okano, M. T. (2021). Um panorama da implementação da lgpd no brasil: uma pesquisa exploratória com 216 profissionais.

Flores, D. A. and Perugachi, R. (2023). A gdpr-compliant risk management approach based on threat modelling and iso 27005. *arXiv preprint arXiv:2306.04783*.

GDPR (2016). Intersoft consulting - general data protection regulation (gdpr). Disponível em `https://https://gdpr-info.eu`.

Hussain, F., Hussain, R., Noye, B., and Sharieh, S. (2020). Enterprise api security and gdpr compliance: Design and implementation perspective. *IT Professional*, 22(5):81–89.

ISO/IEC (2019). Iso/iec 27701:2019 security techniques . Disponível em `https://www.iso.org/standard/71670.html`. Acesso em: 27 abril 2023.

ISO/IEC (2022). Iso 27002: Boas práticas para gestão de segurança da informação. Disponível em `https://www.iso.org/standard/75652.html`. Acesso em: 27 abril 2023.

LGPD (2018). Lei geral de proteção de dados pessoais (lgpd). Disponível em `https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`.

Lima, V. H. (2020). Lgpd análise dos impactos da implementaçao em ambientes corporativos: Estudo de caso.

Lopes, F. and Amaral, M. A. A. (2022). Implementação da lei geral de proteção de dados pessoais (lgpd) em uma instituição sem fins lucrativos, atuante na área da educação básica. *PROJETOS E RELATÓRIOS DE ESTÁGIOS*, 4(1):21–21.

Lugati, L. N. and de Almeida, J. E. (2022). A lgpd e a construção de uma cultura de proteção de dados. *Revista de Direito*, 14(01):01–20.

Marques, L. N. (2020). O mapeamento do modelo data management maturity (dmm) à lei geral de proteção de dados (lgpd).

Menegazzi, D. (2021). Um guia para alcançar a conformidade com a lgpd por meio de requisitos de negócio e requisitos de solução. Master's thesis, Universidade Federal de Pernambuco.

Montolli, C. Â. (2020). Segurança da informação e da transparência e a proteção de dados na administração pública: Lgpd, acesso à informação e os incentivos à inovação e à pesquisa científica e tecnológica no âmbito do estado de minas gerais. *REVISTA ELETRÔNICA DA PGE-RJ*, 3(3).

Okano, M. T., Ferreira, L., dos Santos, H. d. C., and Ursini, E. L. (2021). Lgpd o novo desafio para as organizações: Exemplos de frameworks para diagnosticar este novo cenário. *South American Development Society Journal*, 7(20):380.

Paini, G. S. and Zilles, M. H. B. (2021). A lei geral de proteção de dados: Comentários acerca do propósito e da aplicabilidade. *Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste*, 6:e27804–e27804.

Piurcosky, F. P., Costa, M. A., Frogeri, R. F., and Calegario, C. L. L. (2019). A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de negocios*, 10(23):89–99.

ROCHA, C. P. d., Carneiro, A. V. S., Medeiros, M. V. B., and Melo, A. (2019). Segurança da informação: A iso 27001 como ferramenta de controle para lgpd. *Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará*, 2(3):78–97.

Rodrigues, A. C. and de Paula, A. P. (2022). Prestação dos serviços públicos à luz da lei geral de proteção de dados (lgpd). *Academia de Direito*, 4:1039–1055.

Silva, B. S. d. S. (2021). *O impacto da LGPD no desenho da política de governança de dados nos municípios: o caso de Belo Horizonte*. PhD thesis.

Silva, R. H. d. et al. (2021). Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais.

Teixeira, G. A., da Silva, M. M., and Pereira, R. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*.