Anais do Congresso Brasileiro de Iniciação Científica
(https://periodicos.unisanta.br/COB)

ISSN 2317-1316

FRAMEWORK DE CONFORMIDADE À LGPD INTEGRADO AO CICLO DE VIDA DE DESENVOLVIMENTO DE SOFTWARE (SDLC)

LGPD COMPLIANCE FRAMEWORK INTEGRATED INTO THE SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

Vinícius Barros Santos, João Vitor Rego Muniz

Centro Universitário Unidade de Ensino Superior Dom Bosco (UNDB), Curso de Engenharia de Software
E-mail para contato: barrosv277@gmail.com

RESUMO – Este artigo propõe um framework de conformidade à Lei Geral de Proteção de Dados Pessoais (LGPD) integrado ao Ciclo de Vida de Desenvolvimento de Software (SDLC). A pesquisa, de natureza aplicada, exploratória e bibliográfica, baseou-se em revisão da literatura sobre proteção de dados, Privacy by Design e engenharia de software, mapeando os requisitos da LGPD relevantes ao desenvolvimento e as etapas do SDLC em que devem ser incorporados. O resultado é um framework composto por uma tabela de diretrizes que cruza as sete etapas do SDLC com os princípios da LGPD e do Privacy by Design, um fluxograma e um guia de aplicação, oferecendo às equipes um ponto de partida estruturado para a conformidade legal.

Palavras-chave: LGPD; *Privacy by Design*; SDLC; Desenvolvimento de Software; Proteção de Dados.

ABSTRACT – This paper proposes a compliance framework for the Brazilian General Data Protection Law (LGPD) integrated into the Software Development Life Cycle (SDLC). The applied, exploratory and bibliographic research was based on a literature review on data protection, Privacy by Design and software engineering, mapping the LGPD requirements relevant to software development and the SDLC stages in which they must be incorporated. The result is a framework composed of a guidelines table that crosses the seven SDLC stages with the principles of the LGPD and Privacy by Design, an application flowchart and a usage guide, offering development teams a structured starting point for legal compliance.

Keywords: LGPD; Privacy by Design; SDLC; Software Development; Data Protection.

ISSN 2317-1316

1. INTRODUÇÃO

O crescimento acelerado das tecnologias digitais e a expansão dos sistemas de software nas mais diversas esferas da sociedade têm gerado um volume sem precedentes de dados pessoais coletados, armazenados e processados por organizações públicas e privadas. Nesse contexto, a proteção da privacidade tornou-se um desafio central para o desenvolvimento de software, demandando não apenas soluções técnicas, mas também o alinhamento entre práticas de engenharia e exigências legais.

No Brasil, a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), conhecida como LGPD, representou um marco regulatório significativo ao estabelecer princípios, direitos e obrigações para o tratamento de dados pessoais por parte de controladores e operadores. Em seu artigo 46, a lei determina que medidas de segurança devem ser adotadas desde a fase de concepção dos sistemas, incorporando ao ordenamento jurídico brasileiro o conceito internacionalmente reconhecido de *Privacy by Design* (PbD) (BRASIL, 2018).

Apesar da vigência da LGPD, estudos recentes apontam que muitas equipes de desenvolvimento de software ainda carecem de conhecimento consolidado sobre como garantir a conformidade legal ao longo do Ciclo de Vida de Desenvolvimento de Software (SDLC). Essa lacuna evidencia a necessidade de instrumentos práticos que orientem as equipes de desenvolvimento na incorporação dos requisitos da LGPD em cada etapa do processo de criação de sistemas (REIS, 2023).

Diante disso, este artigo tem como objetivo geral propor um *framework* de conformidade à LGPD integrado ao SDLC, oferecendo diretrizes estruturadas que possibilitem às equipes de desenvolvimento adotar práticas de privacidade desde as fases iniciais de um projeto de software. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos: a) mapear os principais requisitos da LGPD relevantes ao desenvolvimento de software; b) analisar os fundamentos do *Privacy by Design* e sua aplicação no contexto do SDLC; c) identificar as etapas do SDLC nas quais requisitos de privacidade devem ser incorporados; e d) propor um *framework* estruturado que integre a conformidade à LGPD ao ciclo de vida de desenvolvimento de software.

ISSN 2317-1316

A pesquisa justifica-se pela crescente relevância da proteção de dados no contexto do desenvolvimento de software, pelo caráter recente e ainda em processo de regulamentação da LGPD, e pela escassez identificada na literatura de propostas práticas que traduzam as exigências legais em diretrizes aplicáveis ao cotidiano das equipes de desenvolvimento. A criação da Autoridade Nacional de Proteção de Dados (ANPD) e seu poder sancionatório — com multas de até 2% do faturamento da pessoa jurídica, limitadas a R$ 50.000.000,00 por infração — reforça a urgência de instrumentos como o proposto neste trabalho (BRASIL, 2018).

Este artigo está organizado da seguinte forma: a Seção 2 apresenta o referencial teórico, abordando os fundamentos da LGPD, o conceito de *Privacy by Design*, os principais modelos de SDLC e os trabalhos relacionados. A Seção 3 descreve os materiais e métodos adotados. A Seção 4 apresenta os resultados e a discussão, com a descrição completa do *framework* proposto. Por fim, a Seção 5 expõe a conclusão.

2. REFERENCIAL TEÓRICO

a. Lei Geral de Proteção de Dados Pessoais (LGPD)

A crescente digitalização das relações sociais e econômicas trouxe consigo um aumento expressivo na coleta e no processamento de dados pessoais por organizações públicas e privadas. No Brasil, esse movimento culminou na promulgação da Lei n. 13.709, de 14 de agosto de 2018, conhecida como LGPD, que entrou em vigor em agosto de 2020 (DONEDA, 2020).

Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), a LGPD tem como objetivo proteger os direitos fundamentais de liberdade e privacidade dos titulares de dados pessoais. A norma aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio utilizado ou do país onde esteja sediada, desde que o tratamento ocorra no território nacional ou que os dados sejam coletados de pessoas localizadas no Brasil (REIS, 2023).

A lei estrutura o tratamento de dados pessoais em torno de dez princípios fundamentais estabelecidos em seu art. 6º: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Esses

ISSN 2317-1316

princípios constituem a espinha dorsal da norma e devem ser observados por todos os agentes de tratamento, sendo de especial relevância para o desenvolvimento de software, uma vez que sistemas que lidam com dados pessoais precisam ser projetados em conformidade com cada um deles (BRASIL, 2018).

Destaca-se ainda o artigo 46 da LGPD, que determina que medidas de segurança, técnicas e administrativas, devem ser adotadas desde a fase de concepção do produto ou do serviço até a sua execução. Essa determinação incorpora ao texto legal o princípio internacionalmente conhecido como *Privacy by Design* (REIS, 2023).

b. *Privacy by Design*

A abordagem do *Privacy by Design* (PbD), cuja tradução literal seria "a privacidade desde a concepção", surgiu na década de 1990 a partir dos trabalhos da pesquisadora Ann Cavoukian. O conceito foi formalmente apresentado à comunidade científica internacional em 2009 e reconhecido como padrão internacional na 32ª Conferência Internacional de Autoridades de Proteção de Dados e Privacidade, em Jerusalém (CAVOUKIAN, 2010).

A premissa central do PbD é que a privacidade não deve ser tratada como um requisito a ser atendido após a conclusão de um sistema, mas como um elemento estruturante incorporado desde as primeiras fases de concepção de qualquer produto, serviço ou processo que envolva o tratamento de dados pessoais. Essa concepção representa uma mudança significativa na forma como as organizações abordam a privacidade: em vez de tratar a proteção de dados como uma obrigação legal reativa, o PbD propõe que a privacidade seja incorporada proativamente à cultura organizacional e aos processos de desenvolvimento (MELO; ROCKEMBACH; SILVA, 2023).

Cavoukian (2010) estabeleceu sete princípios fundamentais do PbD: a) proatividade e prevenção; b) privacidade como padrão; c) privacidade incorporada ao *design*; d) funcionalidade plena; e) segurança de ponta a ponta; f) visibilidade e transparência; e g) respeito pela privacidade do usuário. No contexto brasileiro, a relevância do PbD foi reforçada com a promulgação da LGPD, cujo artigo 46 incorpora diretamente seus fundamentos, tornando sua adoção uma obrigação legal para os agentes de tratamento de dados (MELO; ROCKEMBACH; SILVA, 2023).

ISSN 2317-1316

c. Ciclo de Vida de Desenvolvimento de Software (SDLC)

O Ciclo de Vida de Desenvolvimento de Software (SDLC) é um conjunto estruturado de fases, atividades e entregas que orientam o processo de criação de sistemas, garantindo que o produto atenda aos requisitos especificados com qualidade e dentro dos prazos estabelecidos (PRESSMAN; MAXIM, 2016). De forma geral, o SDLC é composto por sete etapas fundamentais: planejamento, análise de requisitos, *design*, desenvolvimento, testes, implantação e manutenção.

Ao longo da história da engenharia de software, diferentes modelos de SDLC foram propostos. O modelo cascata, proposto por Royce em 1970, caracteriza-se por uma abordagem sequencial e linear, adequada para projetos com requisitos estáveis. Em resposta às suas limitações, surgiram as metodologias ágeis, formalizadas em 2001 com o Manifesto Ágil, que propõem um desenvolvimento iterativo e incremental. O Scrum, um dos *frameworks* ágeis mais adotados, organiza o trabalho em *sprints* de duas a quatro semanas, com cerimônias regulares que favorecem a adaptação contínua às mudanças de requisitos (SCHWABER; SUTHERLAND, 2020).

Do ponto de vista da conformidade com a LGPD, independentemente do modelo de SDLC adotado, a abordagem do *Privacy by Design* recomenda que considerações sobre privacidade estejam presentes em todas as etapas do ciclo de vida, desde o planejamento até a manutenção, garantindo que a proteção de dados pessoais seja tratada como um requisito fundamental do sistema (REIS, 2023).

d. Trabalhos Relacionados

A produção científica sobre a integração entre legislações de proteção de dados e práticas de engenharia de software tem crescido de forma expressiva, impulsionada especialmente pela entrada em vigor do GDPR na União Europeia e da LGPD no Brasil. Reis (2023) conduziu uma revisão sistemática da literatura com o objetivo de investigar como as leis de privacidade impactam as atividades de engenharia de software. A partir da análise de 11 estudos primários selecionados entre 2.832 trabalhos nas bases ACM, IEEE, ScienceDirect e Springer, o autor identificou que grande parte das pesquisas concentra seus esforços na fase de especificação de requisitos como principal ponto de impacto das legislações de privacidade.

ISSN 2317-1316

O estudo também constatou que equipes frequentemente carecem de conhecimento sobre as exigências legais, dificultando a correta especificação de requisitos de privacidade. Conforme sintetizado pelo próprio autor:

> Há uma baixa familiaridade com textos jurídicos por parte dos engenheiros de software, o que resulta em uma dificuldade de compreender o que deve ser feito para que sistemas estejam em conformidade com leis de privacidade vigentes. Outro achado é a necessidade de haver, em organizações ou em equipes, a presença de uma pessoa com experiência em análise e interpretação de textos legais, para que haja uma redução de ambiguidade e melhoria no processo de especificação de requisitos de privacidade. (REIS, 2023, p. 44)

Melo, Rockembach e Silva (2023) investigaram as possibilidades de pesquisa em torno do *Privacy by Design* no âmbito da Ciência da Informação, identificando a crescente relevância do tema no cenário das legislações de proteção de dados, incluindo a LGPD. Contudo, assim como o trabalho anterior, os autores não avançam para a proposição de diretrizes práticas voltadas ao desenvolvimento de software.

A análise dos trabalhos relacionados permite identificar um padrão recorrente na literatura: embora exista um conjunto consolidado de pesquisas que diagnosticam os impactos das leis de privacidade sobre o desenvolvimento de software, há uma escassez significativa de propostas práticas que integrem esses dois universos de forma estruturada. É precisamente nessa lacuna que o presente trabalho se posiciona.

3. MATERIAIS E MÉTODOS

O presente trabalho caracteriza-se como uma pesquisa de natureza aplicada, uma vez que visa gerar conhecimento voltado à resolução de um problema prático: a ausência de um instrumento estruturado que oriente equipes de desenvolvimento de software na implementação de requisitos de conformidade à LGPD ao longo do SDLC.

Quanto aos objetivos, a pesquisa é classificada como exploratória e descritiva. É exploratória porque busca ampliar o conhecimento sobre um tema ainda em consolidação na literatura, e descritiva por apresentar as características dos fenômenos estudados, estabelecendo relações entre os conceitos de LGPD, *Privacy by Design* e SDLC. Quanto à abordagem, adota-se perspectiva qualitativa, adequada ao objetivo de compreender e interpretar conceitos,

ISSN 2317-1316

princípios e relações entre os elementos teóricos que fundamentam a proposição do *framework* (GIL, 2002).

No que diz respeito aos procedimentos técnicos, foi adotada a pesquisa bibliográfica como método principal. A condução da pesquisa seguiu um processo estruturado em três etapas. Na primeira, foram definidos os termos de busca a partir dos conceitos centrais do trabalho: "LGPD desenvolvimento de software", "*Privacy by Design* SDLC", "proteção de dados engenharia de software" e "*privacy by design software development lifecycle*". Na segunda etapa, as buscas foram realizadas nas bases de dados Google Acadêmico, Portal de Periódicos da CAPES e SciELO, bem como nas obras clássicas de engenharia de software de Sommerville (2011) e Pressman e Maxim (2016), além do texto oficial da Lei n. 13.709/2018.

Na terceira etapa, os materiais encontrados foram avaliados com base nos critérios de seleção previamente definidos. A delimitação temporal da busca privilegiou trabalhos publicados entre 2018 e 2025, período que coincide com a promulgação e entrada em vigor da LGPD. Os critérios de inclusão adotados foram: a) relação direta com os temas de proteção de dados, privacidade e desenvolvimento de software; b) publicação em periódicos científicos revisados por pares ou em canais de conferências da área; e c) disponibilidade do texto completo nas bases consultadas. Foram excluídos trabalhos que abordavam privacidade exclusivamente sob perspectivas jurídicas, sem relação com práticas de engenharia de software.

A partir do material selecionado, a construção do *framework* seguiu as etapas de extração dos requisitos de conformidade presentes na LGPD, mapeamento dos princípios do *Privacy by Design* aplicáveis ao desenvolvimento de software, identificação das etapas do SDLC nas quais esses requisitos devem ser incorporados, e estruturação do *framework* na forma de diretrizes práticas organizadas por fase do ciclo de vida.

4. RESULTADOS E DISCUSSÃO

a. Apresentação do *Framework*

O *framework* de conformidade à LGPD integrado ao SDLC é composto por três elementos principais: a tabela de diretrizes, o fluxograma de aplicação e o guia de uso prático. Sua concepção parte do pressuposto, consolidado pela abordagem do PbD, de que a privacidade

ISSN 2317-1316

deve ser incorporada desde as fases iniciais do desenvolvimento, e não tratada como uma conformidade a ser adicionada ao final do processo (CAVOUKIAN, 2010).

O instrumento destina-se principalmente a equipes de desenvolvimento de software que atuam no contexto brasileiro e que precisam garantir a conformidade de seus sistemas com a LGPD. Pode ser adotado tanto em projetos que seguem metodologias tradicionais, como o modelo cascata, quanto em equipes que utilizam abordagens ágeis, como o Scrum, uma vez que as diretrizes propostas foram estruturadas de forma independente do modelo de desenvolvimento adotado.

b. Tabela de Diretrizes do *Framework*

A tabela de diretrizes constitui o elemento central do *framework*. Ela foi construída a partir do cruzamento entre as etapas do SDLC, os princípios da LGPD estabelecidos em seu artigo 6º e os sete princípios do *Privacy by Design* definidos por Cavoukian (2010). Para cada combinação, foi elaborada uma diretriz prática que orienta a equipe de desenvolvimento sobre as ações concretas a serem adotadas em cada fase do ciclo de vida, conforme apresentado na Tabela 1.

Tabela 1: Diretrizes do framework de conformidade à LGPD integrado ao SDLC

Etapa do SDLC	**Princípio da LGPD**	**Princípio do PbD**	**Diretriz prática**
Planejamento	Finalidade	Proativo e Preventivo	Documentar quais dados pessoais serão coletados, por qual finalidade e qual a base legal utilizada
Planejamento	Responsabilização	Privacidade Incorporada	Designar um responsável pela conformidade à LGPD dentro da equipe desde o início do projeto
Análise de Requisitos	Necessidade	Privacidade como Padrão	Especificar como requisito não funcional a coleta mínima de dados — apenas o estritamente necessário
Análise de Requisitos	Transparência	Visibilidade e Transparência	Definir como o sistema informará ao usuário quais dados serão coletados e como serão utilizados
Design	Segurança	Privacidade Incorporada ao *Design*	Modelar a arquitetura com controle de acesso, criptografia e separação de dados pessoais desde o projeto
Design	Adequação	Funcionalidade Plena	Garantir que o *design* do sistema permita ao titular exercer seus direitos (acesso, correção, exclusão)
Desenvolvimento	Segurança	Segurança de Ponta a Ponta	Implementar criptografia, autenticação e *logs* de acesso aos dados pessoais

ISSN 2317-1316

Etapa do SDLC	Princípio da LGPD	Princípio do PbD	Diretriz prática
Desenvolvimento	Não Discriminação	Funcionalidade Plena	Garantir que dados sensíveis não sejam utilizados para fins discriminatórios no código
Testes	Prevenção	Proativo e Preventivo	Incluir casos de teste específicos para verificar a conformidade com os requisitos de privacidade definidos
Testes	Qualidade dos Dados	Privacidade como Padrão	Verificar se o sistema coleta, armazena e processa apenas os dados necessários conforme especificado
Implantação	Segurança	Segurança de Ponta a Ponta	Garantir que o ambiente de produção aplique todas as medidas de segurança definidas no *design*
Implantação	Responsabilização	Visibilidade e Transparência	Disponibilizar política de privacidade acessível ao usuário antes da coleta de dados
Manutenção	Livre Acesso	Respeito pela Privacidade	Manter mecanismos que permitam ao titular consultar, corrigir ou excluir seus dados a qualquer momento
Manutenção	Prevenção	Proativo e Preventivo	Monitorar e revisar periodicamente as práticas de tratamento de dados, atualizando o sistema conforme mudanças na legislação

Fonte: Elaborado pelo autor (2026).

É importante destacar que as diretrizes apresentadas não são exaustivas, podendo ser adaptadas conforme as especificidades de cada projeto. O objetivo é oferecer um ponto de partida estruturado que reduza a distância entre as exigências legais e as práticas de engenharia de software, lacuna amplamente identificada na literatura (REIS, 2023).

c. Detalhamento das Diretrizes por Etapa

i. Planejamento

A etapa de planejamento é o ponto de partida de qualquer projeto de software e, por essa razão, representa o momento mais crítico para a incorporação da privacidade. É nessa fase que as decisões estruturais do projeto são tomadas, como escopo, recursos, prazos e arquitetura geral do sistema. Ignorar a privacidade nesse momento significa carregar um débito técnico e legal ao longo de todo o desenvolvimento (CAVOUKIAN, 2010).

A primeira diretriz recomenda que a equipe documente, já no planejamento, quais dados pessoais serão coletados pelo sistema, com qual finalidade e com base em qual das hipóteses

ISSN 2317-1316

legais previstas na LGPD. A segunda diretriz prevê a designação de um responsável pela conformidade à LGPD dentro da equipe, profissional que deve ter conhecimento suficiente para identificar situações de risco à privacidade e acionar as partes competentes quando necessário. Reis (2023) identificou que a ausência de profissionais com esse perfil nas equipes é um dos principais fatores que dificultam a conformidade com as leis de privacidade.

ii. Análise de Requisitos

A análise de requisitos é a etapa em que os requisitos de privacidade devem ser formalmente incorporados ao projeto, tratados com o mesmo nível de importância que os requisitos funcionais (REIS, 2023). A primeira diretriz recomenda que a coleta mínima de dados seja especificada como requisito não funcional, alinhada ao princípio da necessidade da LGPD e ao segundo princípio do PbD. A segunda diretriz determina que o sistema defina, ainda nessa fase, como informará ao usuário quais dados estão sendo coletados e de que forma serão utilizados, em conformidade com o princípio da transparência (DONEDA, 2020).

iii. *Design*

A etapa de *design* é onde as decisões técnicas têm maior impacto na proteção dos dados pessoais. A primeira diretriz recomenda que a arquitetura do sistema seja modelada com controle de acesso, criptografia e separação de dados pessoais desde o projeto, alinhada ao terceiro princípio do PbD. A segunda diretriz determina que o *design* garanta ao titular de dados a capacidade de exercer seus direitos previstos na LGPD — acesso, correção e exclusão —, conforme estabelece o artigo 18 da lei (BRASIL, 2018).

iv. Desenvolvimento

A etapa de desenvolvimento é o momento em que as diretrizes de privacidade definidas nas fases anteriores precisam ser efetivamente implementadas. A primeira diretriz recomenda a implementação de criptografia, autenticação robusta e *logs* de acesso aos dados pessoais, fundamentais para a prestação de contas exigida pela LGPD. A segunda diretriz determina que dados pessoais sensíveis não sejam utilizados para fins discriminatórios em nenhuma parte do código, alinhada ao princípio da não discriminação da lei (DONEDA, 2020).

v. Testes

Na etapa de testes, as diretrizes de privacidade definidas nas fases anteriores são verificadas na prática. A primeira diretriz recomenda a inclusão de casos de teste específicos

ISSN 2317-1316

para verificar a conformidade com os requisitos de privacidade, incluindo testes de controle de acesso, criptografia, mecanismos de consentimento e fluxos de exercício de direitos pelo titular. A segunda diretriz determina a verificação de que o sistema coleta apenas os dados estritamente necessários. Reis (2023) identificou que os testes de privacidade ainda são precários na maioria das organizações, o que representa um risco significativo de não conformidade.

vi. Implantação e Manutenção

Na implantação, o software passa a operar com dados reais de usuários reais. A primeira diretriz recomenda que o ambiente de produção aplique todas as medidas de segurança definidas no *design*. A segunda determina que a política de privacidade esteja disponível e acessível ao usuário antes do início da coleta de dados (CAVOUKIAN, 2010).

Na manutenção, frequentemente subestimada pelas organizações, a primeira diretriz recomenda que o sistema mantenha mecanismos que permitam ao titular consultar, corrigir ou excluir suas informações a qualquer momento, sob pena de sanções administrativas. A segunda diretriz determina que as práticas de tratamento de dados sejam revisadas periodicamente, com atualização do sistema sempre que houver mudanças na legislação ou nas diretrizes regulatórias da ANPD (DONEDA, 2020).

d. Fluxograma e Guia de Aplicação do *Framework*

O fluxograma de aplicação apresenta, de forma visual, o caminho percorrido pela equipe ao longo do ciclo de vida do software. O diagrama é estruturado em três colunas: a central representa as etapas do SDLC, enquanto as laterais apresentam os princípios da LGPD e do *Privacy by Design* associados a cada etapa. Após a etapa de testes, o fluxograma apresenta um ponto de decisão que verifica se a conformidade com a LGPD foi atingida — caso não tenha sido, o fluxo retorna ao desenvolvimento para revisão e correção. Uma seta de ciclo contínuo conecta a manutenção ao início do fluxo, indicando que a conformidade não é um estado definitivo, mas um processo permanente (CAVOUKIAN, 2010).

O guia de aplicação orienta como o *framework* deve ser utilizado na prática em cinco passos. O Passo 1 consiste na revisão inicial da tabela de diretrizes antes de iniciar o projeto, identificando os itens aplicáveis ao contexto específico. O Passo 2 trata da incorporação das diretrizes ao documento de planejamento, registrando finalidades, base legal e responsável pela

ISSN 2317-1316

conformidade. O Passo 3 prevê o uso da tabela como *checklist* ao longo de cada etapa do SDLC, garantindo rastreabilidade. O Passo 4 consiste na verificação de conformidade antes da implantação, correspondendo ao ponto de decisão do fluxograma. O Passo 5 estabelece o monitoramento contínuo após a implantação, com revisão periódica recomendada ao menos uma vez por ano ou sempre que houver mudanças relevantes na legislação (DONEDA, 2020).

Os resultados obtidos respondem diretamente à lacuna identificada na literatura: conforme apontado por Reis (2023), nenhuma das organizações brasileiras pesquisadas em sua revisão sistemática utilizava guias ou instrumentos estruturados para garantir a conformidade com a LGPD durante o desenvolvimento de software. O *framework* proposto oferece um ponto de partida prático e fundamentado teoricamente para equipes que precisam adequar seus processos à legislação vigente.

5. CONCLUSÃO

Este artigo propôs um *framework* de conformidade à LGPD integrado ao Ciclo de Vida de Desenvolvimento de Software, e os quatro objetivos específicos foram atendidos: foram mapeados os principais requisitos da LGPD relevantes ao desenvolvimento de software, analisados os fundamentos do *Privacy by Design* e sua conexão com o SDLC, identificadas as etapas do ciclo de vida nas quais requisitos de privacidade devem ser incorporados e proposto um *framework* composto por tabela de diretrizes, fluxograma de aplicação e guia de uso prático. Ao cruzar os dez princípios da LGPD com os sete princípios do *Privacy by Design* e as sete etapas do SDLC, o instrumento traduz obrigações legais em ações técnicas específicas, organizadas de forma sequencial e de fácil consulta, podendo ser adotado tanto em metodologias tradicionais quanto em abordagens ágeis. Como limitações, destacam-se a ausência de validação empírica, uma vez que o *framework* foi construído a partir de revisão bibliográfica e não foi aplicado em projetos reais; o foco exclusivo na LGPD, que pode exigir adaptações para organizações sujeitas a múltiplas legislações; e a possibilidade de publicação de novas diretrizes da ANPD após a conclusão deste trabalho. Como trabalhos futuros, sugerem-se a validação empírica do *framework* em organizações brasileiras de diferentes portes e segmentos, sua expansão para contemplar outros contextos de desenvolvimento, como microsserviços e DevSecOps, e o desenvolvimento de uma ferramenta computacional que automatize a geração de *checklists* personalizados conforme as características de cada projeto.

ISSN 2317-1316

Conclui-se que o *framework* proposto contribui para a disseminação de uma cultura de privacidade no desenvolvimento de software no Brasil, incentivando as equipes a tratarem a privacidade não como uma obrigação burocrática, mas como um valor fundamental a ser considerado em cada decisão técnica ao longo do ciclo de vida do projeto (CAVOUKIAN, 2010).

6. DECLARAÇÃO DE USO DE IA

Durante a elaboração deste trabalho, utilizou-se a ferramenta Claude Opus 5.5 (Anthropic) na etapa de revisão e formatação final, com a finalidade de adequar o texto ao modelo de submissão do 18º Cobric e de condensar o resumo e o *abstract* aos limites exigidos. O conteúdo gerado foi revisado, editado e validado pelos autores, que assumem total responsabilidade pelo texto final.

7. REFERÊNCIAS

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 abr. 2025.

CAVOUKIAN, Ann. Privacy by design: the definitive workshop. *Identity in the Information Society*, v. 3, n. 2, p. 247-251, 2010.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da lei geral de proteção de dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

MELO, Jonas Ferrigolo; ROCKEMBACH, Moisés; SILVA, Armando Malheiro da. Ciência da Informação e *Privacy by Design*: aspectos éticos e possibilidades de pesquisa. *LOGEION*: Filosofia da Informação, Rio de Janeiro, v. 9, n. 2, p. 124-143, mar./ago. 2023.

PRESSMAN, Roger S.; MAXIM, Bruce R. *Engenharia de software*: uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2016.

REIS, Daniel Bruno de Castro. *Como as leis de privacidade e de proteção de dados impactam as atividades de engenharia de software*: uma revisão sistemática da literatura. 2023. 49 f. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

SCHWABER, Ken; SUTHERLAND, Jeff. *The Scrum Guide*. 2020. Disponível em: https://scrumguides.org/scrum-guide.html. Acesso em: 9 abr. 2025.

SOMMERVILLE, Ian. *Engenharia de software*. 9. ed. São Paulo: Pearson Prentice Hall, 2011.