DevSecOps Practices for GDPR, HIPAA or LGPD Compliance in Software Development: A Systematic Review

Denisson S. A. de Freitas
denisson.freitas@dcomp.ufs.br
Universidade Federal de Sergipe (UFS)
São Cristóvão, Sergipe, Brasil

Adicinéia Aparecida de Oliveira
adicineia@dcomp.ufs.br
Universidade Federal de Sergipe (UFS)
São Cristóvão, Sergipe, Brasil

Edward D. Moreno
edward@dcomp.ufs.br
Universidade Federal de Sergipe (UFS)
São Cristóvão, Sergipe, Brasil

Gilton J. F. da Silva
gilton@dcomp.ufs.br
Universidade Federal de Sergipe (UFS)
São Cristóvão, Sergipe, Brasil

Abstract

Context: The current software development scenario requires integrating security and regulatory compliance practices, especially after implementing regulations such as LGPD, GDPR, and HIPAA. **Problem:** There is a lack of frameworks that effectively combine security, regulatory compliance, and continuous software delivery in DevSecOps environments. **Solution:** This study aims to identify and analyze approaches, methods, tools, and frameworks that promote regulatory compliance in DevSecOps practices through a systematic literature review. **IS Theory:** Sociotechnical Theory underpins the analysis, considering the interaction between technical (automated tools and processes) and social (organizational culture and collaborative practices) aspects necessary to effectively implement regulatory compliance. **Method:** A systematic review was carried out following the guidelines for performing systematic literature reviews in software engineering and analyzing 15 primary studies identified in five scientific databases (ACM Digital Library, IEEE Xplore Digital Library, Web of Science, Science Direct and Scopus). **Summarization of Results:** The need for automation of compliance checks, early integration of security practices, and establishing an organizational culture that prioritizes regulatory compliance was identified. **Contributions and Impact on IS:** The study provides an overview of existing practices and frameworks, highlighting the need for a sociotechnical approach that integrates technological and organizational aspects to ensure regulatory compliance in DevSecOps environments, contributing to the advancement of secure software development practices.

CCS Concepts

• **Security and privacy** → **Trust frameworks**; **Social aspects of security and privacy**.

Keywords

DevSecOps, Regulatory Compliance, Software Security, Privacy Protection, Security Integration

1 Introdução

Com o crescente interesse por DevSecOps na indústria de software, a integração de práticas de segurança no ciclo de vida do software, abrangendo tanto o desenvolvimento quanto as operações, tornou-se uma prioridade [31]. No entanto, as práticas de segurança devem ser alinhadas com regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) na União Europeia, e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA, na sigla em inglês) nos Estados Unidos. Essas regulamentações têm um impacto direto na forma como o desenvolvimento e as operações de software são conduzidos, exigindo conformidade em todas as etapas do processo [32, 34].

O paradigma DevSecOps, que integra segurança no DevOps, pode ajudar a promover a conformidade com essas regulamentações ao automatizar testes e validações de segurança durante todo o ciclo de vida do software [31]. Práticas como *shift-left security*, que integram segurança desde as primeiras fases do desenvolvimento, e o uso de automação contínua de testes de conformidade, são consideradas essenciais para garantir a conformidade regulatória [31, 32].

A conformidade com o GDPR, por exemplo, é desafiadora para engenheiros de software, uma vez que a regulamentação foi escrita em termos legais e não técnicos. Isso cria uma barreira significativa para sua implementação prática no desenvolvimento e operações de sistemas [38]. De maneira semelhante, a LGPD no Brasil também apresenta desafios de implementação, com profissionais de Tecnologia da Informação e Comunicação (TIC) relatando falta de conhecimento adequado para garantir conformidade com os princípios da lei, especialmente no que se refere à responsabilização e prestação de contas (*accountability*) [15, 34].

Este estudo contribui significativamente para a academia e a indústria de software ao fornecer uma análise abrangente das práticas que integram DevSecOps com conformidade regulatória, especialmente em um cenário normativo marcado por regulamentações como GDPR, HIPAA e LGPD. A investigação sobre a integração de segurança e conformidade no desenvolvimento e operações de software é essencial, uma vez que a ausência de *frameworks* que conciliem esses aspectos com a entrega contínua representa um desafio para a indústria. Este estudo promove a evolução das práticas de desenvolvimento seguro, destacando a importância da adequação legal e da mitigação de riscos em um ambiente cada vez mais digital e regulamentado.

A originalidade deste estudo é evidenciada pela inexistência de revisões sistemáticas sobre a integração de práticas DevSecOps com conformidade regulatória para as principais regulamentações

globais, conforme identificado na análise da literatura. Ao identificar e analisar abordagens, métodos, ferramentas e *frameworks*, o estudo combina aspectos técnicos, como automação e segurança, com fatores sociais, incluindo cultura organizacional e colaboração, fundamentais para a conformidade. Fundamentado na Teoria Sociotécnica [9, 12, 27], o estudo oferece uma visão holística das práticas existentes, ressaltando a necessidade de uma abordagem integrada que contemple requisitos técnicos e organizacionais.

Para a academia, o estudo identifica lacunas e oportunidades para novas pesquisas, além de aplicar a Teoria Sociotécnica para analisar a interação entre fatores técnicos e sociais na implementação da conformidade regulatória. Para a indústria, os achados oferecem diretrizes práticas para a adoção de práticas como *shift-left security*, automação de testes de conformidade e desenvolvimento de uma cultura organizacional voltada à segurança. Os resultados podem ser utilizados por pesquisadores para propor novos *frameworks* ou aprimorar os existentes, enquanto profissionais de software podem aplicá-los para garantir conformidade com regulamentações, minimizando riscos de violações e penalidades.

Este estudo busca identificar abordagens, métodos, técnicas e *frameworks* que assegurem a conformidade com regulamentações como LGPD, GDPR e HIPAA em práticas DevSecOps. O estudo examina como essas práticas podem ser organizadas para atender às exigências de segurança e requisitos legais sem comprometer a agilidade do DevSecOps, permitindo que equipes de desenvolvimento e operações de software conciliem inovação e conformidade regulatória.

O presente trabalho estrutura-se nas seguintes seções: a Seção 2 apresenta os conceitos teóricos essenciais que fundamentam a integração de práticas DevSecOps com requisitos de conformidade regulatória, discutindo o paradigma DevSecOps e as principais regulamentações de proteção de dados, como GDPR, LGPD e HIPAA. Em seguida, a Seção 3 detalha os procedimentos metodológicos adotados na revisão sistemática da literatura, incluindo as questões de pesquisa, estratégias de busca, critérios de seleção e o processo de análise dos estudos selecionados. A Seção 4 expõe os principais achados da revisão, discutindo as práticas, ferramentas e frameworks identificados, bem como suas implicações para a integração de DevSecOps com conformidade regulatória. A Seção 5 aborda as limitações e possíveis vieses da pesquisa, destacando as ameaças à validade do estudo. Por fim, a Seção 6 sintetiza as principais contribuições do trabalho, apontando direções para pesquisas futuras e destacando a importância de uma abordagem holística que integre aspectos técnicos e organizacionais para garantir a conformidade regulatória em ambientes DevSecOps.

2 Fundamentação Teórica

A fundamentação teórica estabelece definições e conceitos que orientam a análise da integração entre práticas DevSecOps e requisitos de conformidade regulatória. Esta seção apresenta os conceitos essenciais relacionados ao desenvolvimento seguro de software e às regulamentações de proteção de dados, fornecendo embasamento para as análises e conclusões da pesquisa.

2.1 DevSecOps: Integração de segurança no ciclo de vida de desenvolvimento e operações de software

O DevOps surgiu como uma abordagem que integra desenvolvimento e operações de software, promovendo colaboração, automação e responsabilidade compartilhada ao longo do ciclo de vida do desenvolvimento. Conforme destacado por Humble e Molesky [19], Erich et al. [16], de França et al. [14], essa integração visa melhorar a eficiência, a qualidade e a velocidade de entrega de software, alinhando as práticas de TI às demandas dinâmicas do mercado. Além disso, Wiedemann et al. [42] reforçam que o DevOps facilita o alinhamento intra-TI por meio de mecanismos como responsabilidade integrada e conhecimento multidisciplinar, promovendo uma cultura de colaboração e agilidade.

O DevSecOps emerge como uma evolução natural do DevOps, representando uma mudança paradigmática que visa integrar a segurança em cada estágio do ciclo de vida de desenvolvimento e operações de software [11, 17, 32]. Esta abordagem revoluciona o desenvolvimento e operações de software ao incorporar práticas de segurança de forma contínua, tornando-a uma responsabilidade compartilhada entre as equipes de desenvolvimento, segurança e operações de Tecnologia da Informação (TI), em vez de ser uma preocupação isolada ao final do processo [11, 17].

A implementação do DevSecOps caracteriza-se pela automação e integração de controles de segurança no *pipeline* de desenvolvimento e operações de software, permitindo a entrega rápida e segura de software sem comprometer a agilidade do processo [20, 30, 33]. Esta metodologia visa equilibrar a velocidade de entrega com requisitos de segurança, através da automação de testes de segurança estáticos e dinâmicos, monitoramento contínuo e práticas de segurança por design, resultando em software mais resiliente e processos mais eficientes [17, 30, 31].

Um aspecto fundamental do DevSecOps é sua capacidade de transformar atividades de segurança tradicionalmente manuais em processos automatizados e integrados ao fluxo de trabalho de desenvolvimento e operações de software [11, 30]. Esta transformação se manifesta através da implementação de práticas como Segurança como Código (SaC, na sigla em inglês), avaliação contínua de segurança e a integração de ferramentas de teste de segurança nos *pipelines* de entrega contínua (CI/CD), permitindo a identificação e remediação precoce de vulnerabilidades [30].

A adoção do DevSecOps, embora desafiadora, representa uma mudança cultural significativa na TI, que vai além da mera implementação de ferramentas e processos [17]. Esta abordagem requer uma transformação holística que engloba três aspectos centrais: capacidades técnicas, facilitadores culturais e tecnológicos, além de práticas específicas categorizadas em termos de processo, infraestrutura e colaboração [25]. O sucesso desta implementação depende da harmonização entre velocidade de desenvolvimento, segurança e qualidade, resultando em um processo de desenvolvimento e operações mais eficiente, bem como em sistemas de informações e produtos de software mais seguros.

2.2 Regulamentações de proteção de dados

As regulamentações de proteção de dados têm se tornado cada vez mais relevantes no cenário global, como evidenciado pelos dados

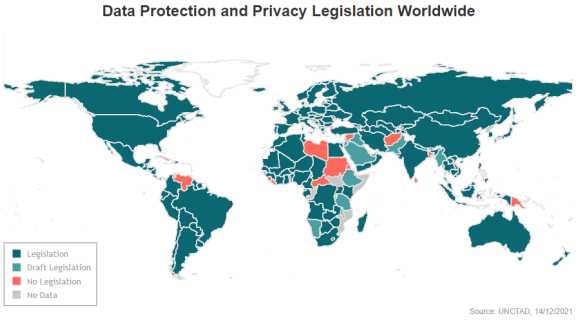
da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, na sigla em inglês) [40], indicam que 134 países do mundo (o equivalente a 71%) já estabeleceram legislações específicas para garantir a proteção de dados e privacidade. Entre os marcos regulatórios pode-se destacar o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, a Lei Geral de Proteção de Dados (LGPD) do Brasil e a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA, na sigla em inglês) dos Estados Unidos. A LGPD, conforme destacado por Passos [29], representa um desafio significativo de conformidade para as empresas , exigindo uma reformulação completa na forma como coletam, armazenam e utilizam dados pessoais durante todo o ciclo de vida das informações.

O GDPR, que serviu de inspiração para a LGPD brasileira, busca estabelecer um equilíbrio entre os direitos individuais à proteção de dados e as necessidades dos setores de pesquisa e negócios de processar essas informações [7]. A LGPD, por sua vez, como observado por Sombra [36], visa reequilibrar as relações de poder, aumentar a transparência e capacitar os titulares de dados em suas interações no ciberespaço, estabelecendo princípios fundamentais como propósito, necessidade, acesso aberto e responsabilidade.

No contexto específico da saúde, a HIPAA estabelece um conjunto abrangente de proteções contra a divulgação não intencional e inadequada de informações pessoais de saúde, incluindo o controle do paciente sobre o uso de suas informações e direitos relacionados às políticas de divulgação [8]. Esta regulamentação se diferencia do GDPR e da LGPD por seu foco exclusivo no setor de saúde, estabelecendo protocolos rigorosos para salvaguardar os riscos associados à atividade médica e à privacidade do paciente. Enquanto o GDPR capacita os indivíduos a exercer controle sobre seus dados pessoais em um sentido mais amplo e define padrões rigorosos para a proteção de dados em todos os setores, a HIPAA concentra-se na confidencialidade, integridade e disponibilidade das informações eletrônicas de saúde (ePHI, na sigla em inglês), especificando controles para lidar com os desafios de segurança no ambiente médico [35].

A harmonização entre estas diferentes regulamentações representa um desafio significativo para organizações globais, especialmente considerando que, segundo a UNCTAD [40], ainda existem disparidades significativas na adoção de legislações de proteção de dados entre diferentes regiões do mundo, com África e Ásia apresentando taxas de adoção de 61% e 57% respectivamente, enquanto os países menos desenvolvidos registram apenas 48% de adoção. Como destacado por Kim [21], a LGPD foi desenvolvida após oito anos de discussão e busca alinhar-se com os padrões internacionais de proteção de dados, especialmente o GDPR europeu, demonstrando uma tendência global de fortalecimento dos direitos individuais sobre dados pessoais, embora 15% dos países ainda não possuam legislação específica e 9% estejam em processo de desenvolvimento de suas regulamentações. A Figura 1 apresenta a distribuição global das legislações de Proteção de Dados e Privacidade, evidenciando as regiões que já adotaram regulamentações específicas e aquelas que ainda estão em fase de desenvolvimento ou sem regulamentação.

Figura 1: Legislação de Proteção de Dados e Privacidade em todo o mundo



Fonte: UNCTAD [40]

3 Metodologia

Foi conduzida uma revisão sistemática da literatura (SLR) para coletar os artigos de pesquisa primária pertinentes a este estudo. Este método é eficaz na identificação, avaliação e análise de artigos relacionados às questões de pesquisa específicas. Dessa forma, uma SLR facilita a compilação de estudos primários sobre um determinado tema. Diferentemente das revisões de literatura não estruturadas, uma SLR segue etapas predefinidas, assegurando um processo metódico e organizado [23].

A metodologia proposta por Kitchenham et al. [23] foi adotada para a condução da busca de artigos. A fim de garantir a eficiência do processo de busca, definiram-se palavras-chave relevantes. Após a realização da busca, gerou-se uma lista preliminar de artigos. Em seguida, aplicaram-se critérios específicos para eliminar aqueles que não se enquadravam no escopo da pesquisa. Os artigos remanescentes passaram por uma leitura completa, durante a qual se aplicou uma Lista de Verificação de Avaliação da Qualidade (QAC, na sigla em inglês). A partir desse processo de refinamento e avaliação qualitativa, obteve-se uma lista final com os artigos primários que respondem adequadamente às questões de pesquisa.

3.1 Questões de pesquisa

As questões de pesquisa tiveram como objetivo delinear os principais questionamentos que orientaram a investigação proposta no estudo. As perguntas formuladas foram relevantes para direcionar a Revisão Sistemática da Literatura (SLR) e contribuíram para o alcance dos objetivos do trabalho de forma estruturada e objetiva. O estudo buscou responder às seguintes questões de pesquisa:

- **Q1:** Existem *frameworks* que integrem práticas de DevSecOps que garantam a conformidade com legislações como LGPD, GDPR ou HIPAA no desenvolvimento e operações de software?
- **Q2:** Quais estratégias, técnicas ou práticas são descritas para garantir que a conformidade regulatória como LGPD, GDPR ou HIPAA seja integrada ao DevSecOps?

3.2 Estratégia e termos de busca

O passo fundamental em uma SLR é definir o protocolo de busca. Após determinar a pergunta de pesquisa, optou-se por usar termos e consultas em bases de publicações para identificar o maior número possível de estudos relevantes. A estratégia de busca eletrônica foi escolhida para evitar vieses e oferecer uma visão holística da pesquisa na área.

Após essa escolha, foi elaborado um conjunto de palavras-chave pertinentes para as pesquisas. Considerando abreviações e sinônimos, foram selecionadas as seguintes palavras-chave: *framework*, DevSecOps, GDPR, *General Data Protection Regulation*, HIPAA, *Health Insurance Portability and Accountability Act*, LGPD e Lei Geral de Proteção de Dados Pessoais. Na Tabela 1, estão apresentados os resultados iniciais dos quais as palavras-chave deste estudo foram extraídas.

Tabela 1: Palavras-chave utilizadas para formar a *string* de busca

Palavra chave	Sinônimos
DevSecOps	"*DevOps Security*"
GDPR	"*General Data Protection Regulation*"
HIPAA	"*Health Insurance Portability and Accountability Act*"
LGPD	"Lei Geral de Proteção de Dados Pessoais"
conformidade	*compliance*
framework	*framework*

As operações lógicas "AND" e "OR" foram empregadas na construção de uma *string* de busca, com o objetivo de refinar os resultados e assegurar a inclusão de estudos relevantes. Por meio dessa *string*, realizou-se uma busca em bases de publicações selecionadas, permitindo recuperar estudos preliminares que atendem aos critérios definidos para o levantamento. A Tabela 2 apresenta a string de busca utilizada.

Tabela 2: *String* utilizada para realizar as buscas nas bases

framework AND DevSecOps AND (GDPR OR "General Data Protection Regulation" OR HIPAA OR "Health Insurance Portability and Accountability Act" OR LGPD OR "Lei Geral de Proteção de Dados Pessoais")

3.3 Bases de buscas

A utilização das bases Scopus e do Web of Science, em conjunto com as bases de publicações de indexação IEEE Xplore Digital Library e ACM Digital Library, é considerada adequada para a condução de uma SLR na área de engenharia de software [22]. A inclusão da base de publicações Science Direct é justificável, uma vez que é reconhecida como uma fonte respeitável e confiável no campo da tecnologia, devido à sua estrutura de revisão por pares e à ampla coleção de artigos disponíveis [37]. Portanto, essas cinco bases foram utilizadas para conduzir esta pesquisa:

- Scopus <http://www.scopus.com>;
- Web of Science <https://www.webofknowledge.com/>;
- IEEE Xplore Digital Library <http://ieeexplore.ieee.org>;
- ACM Digital Library <http://portal.acm.org>;
- Science Direct <http://www.sciencedirect.com>.

3.4 Critérios de inclusão e exclusão

Critérios específicos de inclusão e exclusão foram aplicados para a seleção dos artigos primários, conforme descrito a seguir:

Critérios de Inclusão:

(1) Estudos que abordem a integração de práticas DevSecOps com *frameworks* ou processos que assegurem a conformidade com regulamentos de privacidade de dados no desenvolvimento e operações de software;
(2) Estudos que discutam *frameworks* relacionados ao DevSecOps ou DevOps Security em conformidade com LGPD, GDPR ou HIPAA;
(3) Estudos que proponham técnicas, ferramentas, métodos ou abordagens para a implementação da conformidade regulatória.

Critérios de Exclusão:

(1) Estudos duplicados;
(2) Estudos que não atendam a nenhum dos critérios de inclusão;
(3) Estudos que não sejam artigos científicos;
(4) Estudos que não estejam em português ou inglês.

3.5 Seleção e análise dos artigos preliminares

As buscas foram realizadas em outubro de 2024. Foram encontrados 88 artigos (incluindo duplicados) nas bases de publicações ACM Digital Library, IEEE Xplore Digital Library, Web of Science e Science Direct. A análise foi realizada através da leitura dos títulos, resumos e palavras-chave. Na Tabela 3 podemos verificar a quantidade de artigos encontradas de acordo com cada uma das bases supracitadas.

Tabela 3: Quantidade de artigos encontrados por base de publicações

Bases	Número de Artigos
ACM Digital Library	34
IEEE Xplore Digital Library	1
Web of Science	1
Science Direct	13
Scopus	39

Dos 88 estudos inicialmente identificados, apenas 18 foram considerados possivelmente relevantes para este estudo. Com isso, os 18 artigos foram selecionados para leitura completa, seguida da avaliação por meio de uma Lista de Verificação de Avaliação da Qualidade (QAC, na sigla em inglês), aplicada para examinar de forma sistemática a qualidade dos estudos incluídos nesta SLR. Esse checklist consiste em um conjunto de perguntas ou critérios específicos, empregados para avaliar a robustez e a validade dos estudos analisados. As perguntas utilizadas para essa avaliação foram as seguintes:

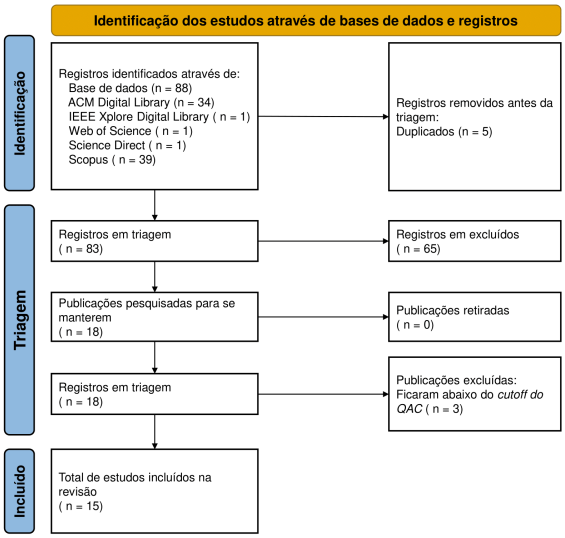
(1) O estudo apresenta a relação entre práticas de desenvolvimento e operações de software e aspectos de conformidade regulatória (como LGPD, GDPR ou HIPAA)?
(2) O estudo fornece informações sobre práticas, métodos, abordagens, ferramentas ou *frameworks* aplicáveis ao desenvolvimento seguro de software em conformidade regulatória?

(3) O estudo apresenta contribuições práticas ou teóricas para auxiliar equipes na implementação de conformidade regulatória em suas práticas de desenvolvimento?
(4) O estudo incentiva a busca por maneiras de integrar conformidade regulatória ao desenvolvimento e operações de software?
(5) O estudo fornece informações sobre benefícios ou desafios enfrentados pela ausência de conformidade regulatória nas práticas de desenvolvimento e operações de software?

As respostas para cada item da avaliação foram categorizadas como "não", "parcialmente" e "sim", com pesos de 0, 1.0 e 2.0, respectivamente, resultando em uma pontuação máxima de 10.0 pontos por estudo. Definiu-se um *cutoff* de 7.0 pontos, equivalente a 70% da pontuação total, para assegurar a seleção de estudos que atendam adequadamente aos critérios de avaliação e apresentem contribuições relevantes ao tema da conformidade regulatória no desenvolvimento e operações de software. Esse valor permite identificar estudos que abordam a maioria dos itens avaliados, priorizando aqueles que exploram métodos, práticas e desafios associados à conformidade regulatória, evitando a inclusão de artigos que tratem o tema de maneira superficial.

Após a aplicação do QAC, 15 artigos foram selecionados para compor a lista final de estudos primários, incluindo apenas aqueles considerados relevantes para esta SLR. Com base no fluxograma Prisma 2020 [28] apresentado na Figura 2, é possível verificar todo o processo sistemático de seleção dos estudos.

Figura 2: Gráfico de prisma com a extração de dados



4 Resultados e Discussão

Os artigos primários selecionados refletem uma distribuição temporal recente, compreendendo publicações entre 2018 e 2024. Destaca-se que 26.67% dos estudos (4 artigos) foram publicados em 2024, evidenciando a contemporaneidade e relevância do tema na literatura científica atual. No período analisado, temos um artigo de 2018 [43], dois de 2019 [1, 26], três de 2020 [2, 10, 13], dois de 2022 [3, 32], três de 2023 [4, 18, 39], e quatro de 2024 [5, 6, 24, 41]. Esta distribuição temporal demonstra um interesse crescente da comunidade científica em investigar aspectos relacionados à segurança no desenvolvimento e operações de software, práticas ágeis e DevSecOps, com especial ênfase em metodologias, e abordagens que englobem a conformidade regulatória.

Esta seção apresenta e discute os principais resultados obtidos a partir das análises dos estudos primários. Inicialmente, a Subseção 4.1 oferece uma visão holística dos estudos. Em seguida, a Subseção 4.2 aborda a conformidade e regulamentações presentes nos estudos. As Subseções 4.3 e 4.4, analisam os resultados em torno das perguntas de pesquisa apresentadas na Subseção 3.1. Finalmente, a 4.5 explora os desafios regulatórios e as contribuições do estudo para a área de Sistemas de Informação.

4.1 Análise holística dos estudos primários

Os estudos primários revelam uma crescente preocupação com a integração de requisitos regulatórios no desenvolvimento e operações de software, especialmente após a implementação de regulamentações como GDPR, LGPD e HIPAA. Ayala-Rivera et al. [6], destacam que, embora novas leis de proteção de dados tenham surgido globalmente, as violações persistem principalmente devido à implementação inadequada ou ausência de controles técnicos robustos. Esta perspectiva é corroborada por Miri et al. [26], que enfatizam que atividades de segurança posteriores são significativamente mais caras e menos eficazes do que incorporar requisitos de segurança nos estágios iniciais do design.

Um aspecto recorrente nos estudos é a necessidade de automatização e ferramentas específicas para garantir conformidade regulatória contínua. Ramaj et al. [32] identificaram que a complexidade dos requisitos regulatórios e a necessidade de automação são obstáculos significativos, enquanto Zheng et al. [43] argumentam que a automação é essencial porque "as pessoas não escalam e as mudanças são constantes". Esta visão é complementada por Casola et al. [10], que propõem uma metodologia quantitativa baseada em Acordos de Nível de Serviços (SLAs, na sigla em inglês) para modelar e avaliar controles de segurança, buscando facilitar a implementação prática de requisitos regulatórios.

A importância da integração precoce de práticas de conformidade no ciclo de desenvolvimento e operações de software é evidenciada em diversos estudos. Anisetti et al. [1] propõem uma metodologia de certificação contínua que incorpora verificações de segurança e conformidade em todas as etapas do desenvolvimento, enquanto Valdés-Rodríguez et al. [41] apresentam uma análise sistemática de estratégias para integração de práticas de segurança em desenvolvimento ágil, com foco especial em pequenas e médias empresas. Ardo et al. [4] complementam essa visão ao destacar as dificuldades específicas enfrentadas em diferentes contextos organizacionais.

Os estudos convergem na identificação de benefícios e desafios da conformidade regulatória. Ayala-Rivera et al. [6] desenvolveram o SoCo, uma ferramenta semi-automatizada que auxilia organizações a alcançarem conformidade com os Princípios de Proteção de Dados do GDPR através da evolução controlada do software. Ardagna et al. [3] propõem uma metodologia baseada em algoritmo genético para otimizar a integração de requisitos de certificação no processo de desenvolvimento, destacando que o custo da não conformidade

pode ser significativamente maior que o investimento em uma abordagem proativa.

Os estudos enfatizam a necessidade de uma mudança cultural nas organizações para a efetiva implementação da conformidade regulatória. Zheng et al. [43] argumentam que a segurança deve começar desde o início do desenvolvimento e continuar durante todo o processo de implantação, envolvendo todos na organização. Essa visão é reforçada por Daoudagh et al. [13], que propõem diretrizes para desenvolvimento contínuo e testes de controles de acesso, elemento crucial para conformidade regulatória, destacando a importância de uma abordagem holística que combine aspectos técnicos e organizacionais.

A análise dos resultados revela que os desafios e benefícios apontados nos estudos, no que tange à integração de práticas de DevSecOps visando garantir conformidade regulatória nas atividades de desenvolvimento e operações de software, contemplam várias questões técnicas, sociais e de negócios. Esses aspectos precisam ser considerados na implementação de sistemas de informações, conforme abordado na Teoria Sociotécnica. A Teoria Sociotécnica, conforme Bostrom e Heinen [9], destaca a importância da interação entre os elementos técnicos (como automação e ferramentas de segurança) e os aspectos sociais (como cultura organizacional e colaboração entre equipes) para o sucesso da implementação de sistemas complexos. Clegg [12] reforça que a otimização conjunta dos subsistemas técnico e social é essencial para maximizar o desempenho organizacional, o que se alinha com a necessidade de integrar práticas de segurança e conformidade desde as fases iniciais do desenvolvimento.

Por fim, Mumford [27] argumenta que a implementação de sistemas de informação deve considerar não apenas a eficiência técnica, mas também o impacto social e organizacional, promovendo uma cultura de colaboração e responsabilidade compartilhada. Portanto, a integração de práticas de DevSecOps com conformidade regulatória não pode ser vista apenas como uma questão técnica, mas também como uma transformação cultural e organizacional que exige a harmonização entre tecnologia, processos e pessoas, conforme proposto pela Teoria Sociotécnica.

4.2 Análise sobre a conformidade regulatória presente nos estudos primários

A análise das regulamentações abordadas nos artigos primários revela um foco expressivo na conformidade com o GDPR, a regulamentação mais citada, indicando sua relevância na literatura sobre segurança e desenvolvimento de software. Esse destaque reflete a centralidade do GDPR como referência para políticas de proteção de dados, especialmente na União Europeia, influenciando diretrizes globais sobre privacidade e segurança digital [1, 3, 6, 24]. Em contraste, a LGPD brasileira é mencionada principalmente como um exemplo comparativo, contextualizando-a em relação a outras regulamentações internacionais [6]. Esse enfoque comparativo sugere um interesse acadêmico na compreensão de similaridades e diferenças entre normas nacionais e internacionais, apontando para a relevância da harmonização de políticas em um cenário global de proteção de dados.

A conformidade com regulamentações como HIPAA, PCI DSS (*Payment Card Industry Data Security Standard*) e NIS Directive (*Network and Information Security Directive*) é abordada em parte dos artigos, que tratam de requisitos de segurança específicos para setores como saúde e finanças, destacando a importância de normas setoriais para a proteção de informações sensíveis [10, 13, 26, 43]. Adicionalmente, o uso de normas regionais ou setoriais, como a Diretiva DORA (*Digital Operational Resilience Act*) da União Europeia, CCPA (*California Consumer Privacy Act*) dos Estados Unidos, e NDPR (*Nigeria Data Protection Regulation*) da Nigéria, demonstra a diversidade de regulamentações aplicáveis em contextos geográficos e operacionais variados [4, 32, 41]. Parte dos estudos referem-se a essas regulamentações como exemplos ilustrativos ou referências comparativas, sugerindo que a conformidade regulatória é um tema de interesse geral na literatura, mesmo quando a pesquisa não se limita a regulamentações específicas. Dessa forma, observa-se que a conformidade regulatória representa um importante componente nas práticas de desenvolvimento seguro, sendo tratada tanto em abordagens específicas quanto em análises amplas de governança e proteção de dados.

4.3 Resposta da questão de pesquisa 1

Foram identificadas 11 tecnologias (incluindo frameworks, abordagens, estratégias, técnicas, métodos, ferramentas e processos) que buscam integrar práticas de DevSecOps visando garantir conformidade regulatória nas atividades de desenvolvimento e operações de software. Essas tecnologias foram extraídas dos estudos primários analisados e são sumarizadas na Tabela 4, que apresenta uma breve descrição de cada uma e suas respectivas referências.

Embora existam diversas abordagens e *frameworks* propostos, não há uma solução única que garanta completamente a conformidade com todas as legislações mencionadas. A conformidade regulatória no desenvolvimento de software é um processo contínuo que requer a integração de práticas de segurança e privacidade desde o início do ciclo de desenvolvimento, automação de verificações e testes, e uma cultura organizacional que priorize a conformidade.

4.4 Resposta da questão de pesquisa 2

A integração da conformidade regulatória com legislações como LGPD, GDPR ou HIPAA no contexto do DevSecOps é um desafio complexo que requer abordagens multifacetadas. Anisetti et al. [1] propõem uma metodologia de certificação contínua que incorpora verificações de segurança e conformidade em todas as etapas do desenvolvimento, destacando a importância de uma abordagem holística. Esta metodologia enfatiza a necessidade de *shift-left security*, ou seja, a incorporação de práticas de segurança e conformidade desde as fases iniciais do ciclo de desenvolvimento, alinhando-se com os princípios fundamentais do DevSecOps.

Uma importante estratégia para garantir a conformidade regulatória no DevSecOps é a automação de processos de verificação e teste. Zheng et al. [43] descrevem a implementação de um ambiente seguro quase isolado na AWS, fundamentado em princípios de segurança DevOps, que utiliza *pipelines* automatizados para entrega contínua (CI/CD). Esta abordagem não apenas aumenta a eficiência do desenvolvimento, mas também reduz significativamente o risco de erros humanos que poderiam levar a violações de conformidade. Complementarmente, Ramaj et al. [32] discutem a importância de ferramentas de teste de conformidade como Chef InSpec e RedHat

Tabela 4: Tecnologias identificadas para integração de DevSecOps e conformidade regulatória

Tecnologia	Referência
Metodologia de certificação contínua e *framework* DevOps	Anisetti et al. [1]
Abordagem SoCo para conformidade com GDPR	Ayala-Rivera et al. [6]
Ferramentas de teste de conformidade (Chef InSpec, RedHat OpenScap)	Ramaj et al. [32]
Framework COMET	Ramaj et al. [32]
Ambiente seguro quase isolado na AWS com automação de processos para conformidade HIPAA	Zheng et al. [43]
Metodologia SSDE (*Security SLA-based Security-by-Design*)	Casola et al. [10]
Diretrizes para integração de desenvolvimento e testes contínuos em DevOps	Daoudagh et al. [13]
Práticas de *Compliance as Code*	Ramaj et al. [32]
Práticas de *shift-left security*	Anisetti et al. [1]
Práticas de *privacy by design*	Ayala-Rivera et al. [6]
Programas de treinamento e conscientização para conformidade regulatória	Daoudagh et al. [13]

OpenScap, além de práticas de *Compliance as Code*, que permitem a codificação e automação de requisitos de conformidade.

A integração de práticas *privacy by design* é outra técnica essencial para garantir conformidade regulatória no DevSecOps. Ayala-Rivera et al. [6] propõem o SoCo, uma abordagem semi-automatizada que auxilia organizações a alcançarem conformidade com o GDPR através da evolução de software. Esta abordagem enfatiza a importância de integrar controles técnicos de privacidade e segurança no design do software desde o início do processo de desenvolvimento. De forma similar, Casola et al. [10] apresentam a metodologia SSDE, que inclui modelos, ferramentas e processos automatizados para análise de risco e avaliação de segurança, permitindo uma abordagem proativa à conformidade regulatória.

A conformidade regulatória no DevSecOps não é apenas uma questão técnica, mas também cultural. Daoudagh et al. [13] fornecem diretrizes gerais para integrar desenvolvimento e testes contínuos em um processo DevOps, enfatizando a necessidade de uma mudança de mentalidade em toda a organização. Esta visão é corroborada por Zheng et al. [43], que destacam a importância de envolver todos os membros da equipe na segurança e conformidade, promovendo uma cultura onde estas preocupações são responsabilidade de todos. Assim, além das estratégias técnicas, é importante implementar programas de treinamento, conscientização e responsabilidade compartilhada para garantir que a conformidade regulatória seja verdadeiramente integrada ao DevSecOps.

4.5 Desafios e contribuições para área de SI

A área de Sistemas de Informação (SI) enfrenta desafios significativos diante da crescente complexidade regulatória e da necessidade de integrar práticas de segurança e conformidade no desenvolvimento e operações de software. A implementação de regulamentações como a LGPD, GDPR e HIPAA exige que as organizações adotem abordagens mais robustas e proativas, capazes de garantir a privacidade e a segurança dos dados desde as fases iniciais do ciclo de desenvolvimento e operações de software. Nesse contexto, a integração de práticas de DevSecOps com requisitos de conformidade regulatória surge como um caminho promissor, mas também desafiador, pois demanda mudanças culturais, técnicas e organizacionais. A automação de processos de verificação e teste, aliada à adoção de práticas como *privacy by design*, representa um avanço importante, mas sua implementação efetiva requer a superação de barreiras como a resistência à mudança e a falta de expertise em conformidade regulatória.

As contribuições deste estudo para a área de SI são evidentes ao buscar frameworks e abordagens que integram DevSecOps com as demandas das regulamentações vigentes. Ao promover a conformidade regulatória como parte intrínseca do desenvolvimento e operações de software, o estudo oferece um caminho para reduzir riscos de violações de dados e aumentar a confiança dos usuários. Adicionalmente, a análise comparativa entre diferentes frameworks e abordagens, bem como a validação de sua eficácia em contextos organizacionais reais, pode fornecer *insights* valiosos para a comunidade acadêmica e profissional. Esses avanços não apenas fortalecem a segurança e a privacidade no desenvolvimento e operações de software, mas também contribuem para a criação de uma cultura organizacional mais consciente e preparada para os desafios da era digital.

Por fim, os impactos dos sistemas sociotécnicos, decorrentes da inter-relação entre LGPD, GDPR, HIPAA e práticas de DevSecOps, evidenciam a importância de uma abordagem holística que considere tanto aspectos técnicos quanto humanos. Este estudo destaca a necessidade de equilibrar a automação e a eficiência com a sensibilização e capacitação dos profissionais, garantindo que a conformidade regulatória seja internalizada como um valor organizacional.

5 Ameaças à validade

De acordo com Zhou et al. [44], uma revisão sistemática da literatura (SLR, na singla em inglês) em engenharia de software pode enfrentar diversas ameaças à sua validade. Os autores identificam ameaças relacionadas às validades de construto, interna, externa e de conclusão, que podem ocorrer nas fases de planejamento, condução e relato da revisão. Entre as principais ameaças, destacam-se: especificação inadequada do protocolo, termos de busca incompletos, viés na seleção e extração de dados, informações incompletas nos estudos primários, generalização limitada e síntese de dados insatisfatória. Essas ameaças têm o potencial de comprometer a qualidade e confiabilidade dos resultados da revisão sistemática. Portanto, ao se desenvolver este estudo, buscou-se identificar e mitigar essas ameaças de forma proativa em todas as fases da pesquisa,

a fim de aumentar o rigor metodológico e a validade das conclusões obtidas.

Entre os aspectos identificados que podem impactar a validade da revisão, destaca-se a limitação na formulação da *string* de busca. A *string* utilizada restringiu-se ao uso do termo *framework* para identificar estudos relevantes, sem incluir sinônimos ou termos relacionados, como "práticas", "técnicas", "métodos", "estratégias" ou "processos". Essa decisão pode ter influenciado na quantidade e diversidade de trabalhos recuperados, uma vez que a literatura sobre DevSecOps e conformidade com regulamentações de proteção de dados pode ser descrita utilizando diferentes terminologias.

6 Considerações Finais

Para atingir o objetivo deste estudo, foi realizada uma revisão sistemática da literatura (SLR, na sigla em inglês). Inicialmente, definiu-se um protocolo de busca, incluindo a seleção de palavras-chave relevantes e a formulação de uma *string* de busca. Em seguida, conduziu-se uma busca sistemática em cinco bases de publicações acadêmicas reconhecidas: Scopus, Web of Science, IEEE Xplore Digital Library, ACM Digital Library e Science Direct. Esta abordagem permitiu uma cobertura ampla e diversificada da literatura existente sobre o tema.

Após a identificação inicial de 88 artigos, foi aplicado um processo de triagem com base em critérios de inclusão e exclusão previamente definidos. Esse processo resultou na seleção de 18 artigos para leitura completa. Em seguida, utilizou-se uma Lista de Verificação de Avaliação da Qualidade (QAC) para avaliar a relevância e a qualidade dos estudos selecionados. Esta etapa garantiu que apenas os estudos mais relevantes e consistentes fossem incluídos na análise final, resultando em um conjunto de 15 artigos primários. A análise detalhada desses artigos possibilitou a identificação de tendências, abordagens inovadoras e desafios na integração de práticas de DevSecOps com requisitos de conformidade regulatória.

A metodologia empregada nesta SLR seguiu as diretrizes propostas por Kitchenham et al. [23], reconhecidas como padrão na condução de revisões sistemáticas. Este método estruturado incluiu a definição clara de questões de pesquisa, a elaboração de um protocolo de busca abrangente, a aplicação de critérios de seleção bem definidos e a utilização de uma ferramenta de avaliação de qualidade. A abordagem sistemática adotada visou minimizar vieses e garantir a reprodutibilidade do estudo, aumentando assim a confiabilidade e validade dos resultados obtidos.

Apesar do rigor metodológico aplicado, é importante reconhecer potenciais limitações que podem afetar a validade deste estudo. Uma possível ameaça à validade de construto reside na definição das palavras-chave e na formulação da *string* de busca, que podem não ter capturado todos os estudos relevantes. A validade interna pode ser afetada por vieses na seleção e extração de dados, enquanto a validade externa pode ser limitada pela generalização dos resultados, considerando o foco específico em certas regulamentações. Adicionalmente, a síntese dos dados pode ser influenciada pela interpretação subjetiva dos pesquisadores, representando uma ameaça à validade de conclusão. Reconhecer estas limitações é importate para uma avaliação crítica dos resultados obtidos nesta pesquisa e para orientar futuras pesquisas na área.

A análise sistemática da literatura realizada neste estudo fornece insights valiosos sobre a integração da conformidade regulatória com as práticas de DevSecOps. A análise de 15 estudos primários revela uma preocupação crescente com a incorporação de requisitos normativos e de segurança no desenvolvimento e operações de software, destacando a necessidade de automação, integração antecipada de práticas de conformidade e uma mudança cultural nas organizações. O estudo identifica 11 tecnologias, incluindo frameworks, abordagens, ferramentas e práticas, destinadas a garantir a conformidade normativa, tais como metodologias de certificação contínua, ferramentas semiautomatizadas, práticas de segurança por projeto (privacy by design) e estratégias de shift-left security. Essas descobertas contribuem para o avanço das práticas de desenvolvimento de software seguro, enfatizando a importância de uma abordagem holística que integre aspectos tecnológicos e organizacionais para garantir a conformidade regulatória em ambientes DevSecOps.

A Teoria Sociotécnica, conforme discutida ao longo do estudo, reforça a necessidade de equilibrar os aspectos técnicos (como automação e ferramentas de segurança) com os aspectos sociais (como cultura organizacional e colaboração entre equipes). Essa abordagem é essencial para a implementação eficaz de sistemas de informação que atendam às demandas regulatórias, como GDPR, LGPD e HIPAA, ao mesmo tempo em que promovem a agilidade e a inovação no desenvolvimento de software. A integração desses elementos técnicos e sociais, conforme proposto pela Teoria Sociotécnica, é fundamental para superar os desafios de conformidade e segurança em um cenário cada vez mais regulamentado.

Para a área de Sistemas de Informação (SI), este estudo oferece contribuições significativas ao destacar a importância de uma abordagem integrada que combine automação, práticas de segurança e mudanças culturais. Ao oferecer diretrizes práticas para organizações que buscam alinhar inovação tecnológica com exigências legais e de segurança, o estudo reforça a importância de uma cultura organizacional que internalize a conformidade e a segurança como prioridades.

Para concluir o trabalho e fortalecer suas contribuições, propõe-se a realização de uma análise comparativa mais aprofundada entre os *frameworks* e abordagens identificados, avaliando sua eficácia em diferentes contextos organizacionais. Sugere-se também a condução de estudos de caso em ambientes reais de desenvolvimento e operações de software para validar a aplicabilidade das práticas e *frameworks* identificados. Adicionalmente, recomenda-se a expansão do escopo da pesquisa para incluir outras regulamentações emergentes e explorar as implicações das práticas de DevSecOps em setores específicos, como saúde e finanças. Por fim, a elaboração de um guia prático ou *framework* para implementação de práticas DevSecOps em conformidade com regulamentações de proteção de dados poderia oferecer valor significativo para profissionais e organizações na área de desenvolvimento de software.

Referências

[1] Marco Anisetti, Claudio A. Ardagna, Filippo Gaudenzi, and Ernesto Damiani. 2019. A Continuous Certification Methodology for DevOps. In *Proceedings of the 11th International Conference on Management of Digital EcoSystems*. 205–212.

[2] Nalin Asanka Gamagedara Arachchilage and Mumtaz Abdul Hameed. 2020. Designing a Serious Game: Teaching Developers to Embed Privacy Into Software

Systems. In *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*. 7–12.
[3] Claudio A. Ardagna, Nicola Bena, and Ramon Martín De Pozuelo. 2022. Bridging the Gap Between Certification and Software Development. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–10.
[4] Abdulhamid A. Ardo, Julian M Bass, and Tarek Gaber. 2023. Implications of Regulatory Policy for Building Secure Agile Software in Nigeria A Grounded Theory. *The Electronic Journal of Information Systems in Developing Countries* 89, 6 (2023), e12285.
[5] Cláudia Ascenção, Henrique Teixeira, João Gonçalves, and Fernando Almeida. 2024. Large-scale Agile Security Practices in Software Engineering. *Information & Computer Security* (2024).
[6] Vanessa Ayala-Rivera, A Omar Portillo-Dominguez, and Liliana Pasquale. 2024. GDPR Compliance Via Software Evolution: Weaving Security Controls in Software Design. *Journal of Systems and Software* (2024), 112144.
[7] H. Bentzen and Njl Hstmlingen. 2019. Balancing Protection and Free Movement of Personal Data: The New European Union General Data Protection Regulation. *Annals of Internal Medicine* 170 (2019), 335–337. https://doi.org/10.7326/M18-2782
[8] B. Blechner and Adam Butera. 2002. Health Insurance Portability and Accountability Act of 1996 (HIPAA): a provider's overview of new privacy regulations. *Connecticut medicine* 66 2 (2002), 91–5.
[9] Robert P Bostrom and J Stephen Heinen. 1977. MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS quarterly* (1977), 17–32.
[10] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, and Umberto Villano. 2020. A Novel Security-by-Design Methodology: Modeling and Assessing Security by SLAs with a Quantitative Approach. *Journal of Systems and Software* 163 (2020), 110537.
[11] Tao Chen and Haiyan Suo. 2022. Design and Practice of Security Architecture via DevSecOps Technology. *2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS)* (2022), 310–313. https://doi.org/10.1109/ICSESS54813.2022.9930212
[12] Chris W Clegg. 2000. Sociotechnical principles for system design. *Applied ergonomics* 31, 5 (2000), 463–477.
[13] Said Daoudagh, Francesca Lonetti, and Eda Marchetti. 2020. Continuous development and testing of access and usage control: A systematic literature review. In *Proceedings of the 2020 European Symposium on Software Engineering*. 51–59.
[14] Breno B Nicolau de França, Helvio Jeronimo, and Guilherme Horta Travassos. 2016. Characterizing DevOps by hearing multiple voices. In *Proceedings of the XXX Brazilian Symposium on Software Engineering*. 53–62.
[15] Edna Dias Canedo, Angelica Toffano Seidel Calazans, Eloisa Toffano Seidel Masson, Pedro Henrique Teixeira Costa, and Fernanda Lima. 2020. Perceptions of ICT practitioners regarding software privacy. *Entropy* 22, 4 (2020), 429.
[16] Floris Erich, Chintan Amrit, and Maya Daneva. 2014. A mapping study on cooperation between information system development and operations. In *International Conference on Product-Focused Software Process Improvement*. Springer, 277–280.
[17] Akanksha Gupta. 2022. An Integrated Framework for DevSecOps Adoption. *arXiv preprint arXiv:2207.04093* (2022).
[18] Rogelio Hernández, Begoña Moros, and Joaquín Nicolás. 2023. Requirements Management in DevOps Environments: A Multivocal Mapping Study. *Requirements Engineering* 28, 3 (2023), 317–346.
[19] Jez Humble and Joanne Molesky. 2011. Why enterprises must adopt devops to enable continuous delivery. *Cutter IT Journal* 24, 8 (2011), 6.
[20] Zalialetdzinau Kanstantsin. 2022. Multivocal Literature Review on the Security of DevSecOp. *Asian Journal of Research in Computer Science* (2022). https://doi.org/10.9734/ajrcos/2022/v14i230329
[21] Hansol Kim. 2022. Legislative Harmonization of Brazilian Data Protection Law with EU GDPR: A Comparative Study on the EU GDPR and Brazil's LGPD. *Center for Legislative Studies, Gyeongin National University of Education* (2022). https://doi.org/10.58555/li.2022.2.105
[22] Barbara Kitchenham and Pearl Brereton. 2013. A systematic review of systematic review process research in software engineering. *Information and software technology* 55, 12 (2013), 2049–2075.
[23] Barbara Kitchenham, Stuart Charters, et al. 2007. Guidelines for performing systematic literature reviews in software engineering.
[24] Felix Lange and Immanuel Kunz. 2024. Evolution of Secure Development Lifecycles and Maturity Models in the Context of Hosted Solutions. *Journal of Software: Evolution and Process* (2024), e2711.
[25] Runfeng Mao, He Zhang, Qiming Dai, Huang Huang, Guoping Rong, Haifeng Shen, Lianping Chen, and Kaixiang Lu. 2020. Preliminary Findings about DevSecOps from Grey Literature. *2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS)* (2020), 450–457. https://doi.org/10.1109/QRS51102.2020.00064
[26] Mina Miri, C. Amir Pourafshar, Pooya Mehregan, and Nathanael Mohammed. 2019. Bridging the Gap Between Policies and Execution in an Agile Environment. *Governance of IT, OT and IoT, ISACA JOURNAL* 4 (2019).
[27] Enid Mumford. 2003. *Redesigning human systems*. IGI Global.
[28] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, et al. 2023. A Declaração PRISMA 2020: Diretriz Atualizada para Relatar Revisões Sistemáticas. *Revista Panamericana de Salud Publica* 46 (2023), e112.
[29] Khyara F. Passos. 2021. Compliance with Brazil's New Data Privacy Legislation: What Us Companies Need to Know. *Social Science Research Network* (2021). https://doi.org/10.2139/SSRN.3777357
[30] Agung Maulana Putra and Herman Kabetta. 2022. Implementation of DevSecOps by Integrating Static and Dynamic Security Testing in CI/CD Pipelines. In *2022 IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM)*. IEEE, 1–6.
[31] R. Rajapakse, Mansooreh Zahedi, M. Babar, and Haifeng Shen. 2021. Challenges and solutions when adopting DevSecOps: A systematic review. *ArXiv* abs/2103.08266 (2021). https://doi.org/10.1016/j.infsof.2021.106700
[32] Xhesika Ramaj, Mary Sánchez-Gordón, Vasileios Gkioulos, Sabarathinam Chockalingam, and Ricardo Colomo-Palacios. 2022. Holding On to Compliance While Adopting DevSecOps: An SLR. *Electronics* 11, 22 (2022), 3707.
[33] Thorsten Rangnau, Remco v. Buijtenen, F. Fransen, and F. Turkmen. 2020. Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines. *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)* (2020), 145–154. https://doi.org/10.1109/EDOC49727.2020.00026
[34] Lucas Dalle Rocha, Geovana Ramos Sousa Silva, and Edna Dias Canedo. 2023. Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*. 1352–1361.
[35] Wasim Fathima Shah. 2023. Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA. *International Journal for Research in Applied Science and Engineering Technology* (2023). https://doi.org/10.22214/ijraset.2023.55551
[36] Thiago Luís Santos Sombra. 2020. The General Data Protection Law in Brazil: What Comes Next? *Global Privacy Law Review* (2020). https://doi.org/10.54648/gplr2020083
[37] Emrah Soykan and Huseyin Uzunboylu. 2015. New trends on mobile learning area: The review of published articles on mobile learning in science direct database. *World Journal on Educational Technology* 7 (2015), 31–41. https://doi.org/10.18844/WJET.V7I1.22
[38] Damian A Tamburri. 2020. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems* 91 (2020), 101469.
[39] Theodoros Theodoropoulos, Luis Rosa, Chafika Benzaid, Peter Gray, Eduard Marin, Antonios Makris, Luis Cordeiro, Ferran Diego, Pavel Sorokin, Marco Di Girolamo, et al. 2023. Security in Cloud-Native Services: A Survey. *Journal of Cybersecurity and Privacy* 3, 4 (2023), 758–793.
[40] UNCTAD. 2021. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 23 out. 2024.
[41] Yolanda Valdés-Rodríguez, Jorge Hochstetter-Diez, Mauricio Diéguez-Rebolledo, Ana Bustamante-Mora, and Rodrigo Cadena-Martínez. 2024. Analysis of Strategies for the Integration of Security Practices in Agile Software Development: A Sustainable SME Approach. *IEEE Access* (2024).
[42] Anna Wiedemann, Manuel Wiesche, Heiko Gewald, and Helmut Krcmar. 2020. Understanding how DevOps aligns development and operations: a tripartite model of intra-IT alignment. *European Journal of Information Systems* 29, 5 (2020), 458–473.
[43] Erkang Zheng, Phil Gates-Idem, and Matt Lavin. 2018. Building a Virtually Air-Gapped Secure Environment in AWS: With Principles of DevOps Security Program and Secure Software Delivery. In *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security*. 1–8.
[44] Xin Zhou, Yuqin Jin, He Zhang, Shanshan Li, and Xin Huang. 2016. A Map of Threats to Validity of Systematic Literature Reviews in Software Engineering. In *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 153–160.