UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
PROGRAMA DE GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

MANOEL ALVES XAVIER NETO

Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software

Recife

2025

MANOEL ALVES XAVIER NETO

Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software

Trabalho apresentado ao Programa de Graduação em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Área de Concentração: *Privacy Standards* e desenvolvimento de *software*

Orientador (a): Prof.ª Jéssyka Flavyanne Ferreira Vilela

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Xavier Neto, Manoel Alves.
Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software / Manoel Alves Xavier Neto. - Recife, 2025.
35 p. : il., tab.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Engenharia da Computação - Bacharelado, 2025.
Inclui referências, apêndices.

1. Privacidade. 2. Padrões de privacidade. 3. Privacy Standards. 4. Engenharia de privacidade. 5. Desenvolvimento de software. I. Vilela, Jéssyka Flavyanne Ferreira. (Orientação). II. Título.

000 CDD (22.ed.)

MANOEL ALVES XAVIER NETO

Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software

Trabalho apresentado ao Programa de Graduação em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do grau de Bacharel em Engenharia da Computação. Área de concentração: *Privacy Standards* e desenvolvimento de *software*.

.

Aprovado em: 14/04/2025.

BANCA EXAMINADORA

_____
Prof.ª Dr.ª Jessyka Flavyanne Ferreira Vilela (Orientadora)
Universidade Federal de Pernambuco - UFPE

_____
Prof.ª Dr.ª Carla Taciana Lima Lourenço Silva Schuenemann (Examinadora Interna)
Universidade Federal de Pernambuco - UFPE

_____
Prof.ª Dr.ª Mariana Maia Peixoto (Examinadora Externa)
Universidade de Pernambuco - UPE

Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software

Manoel Alves Xavier Neto[1], **Jéssyka Vilela**[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Av. Jorn. Aníbal Fernandes, s/n – 50740-560 – Recife – PE – Brasil

{maxn,jffv}@cin.ufpe.br

Abstract. *The General Data Protection Law (LGPD) establishes the need for privacy standards, but its practical implementation faces challenges in Brazil, including the lack of technical resources, specialized knowledge and clear references for the adoption of comprehensive frameworks, causing organizations to prioritize immediate operational solutions over systemic strategies. To investigate this scenario, a survey was conducted with 31 Brazilian developers, analyzing practices, use of tools and challenges in compliance with the LGPD. The survey results revealed contextual gaps, validated global challenges with local particularities, and explained practical guidelines.*

Resumo. *A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece a necessidade de normas de privacy, mas sua implementação prática enfrenta desafios no Brasil, incluindo a carência de recursos técnicos, de conhecimento especializado e de referências claras para adoção de frameworks abrangentes, provocando as organizações a priorizarem soluções operacionais imediatas em detrimento de estratégias sistêmicas. Para investigar esse cenário, foi feita uma pesquisa conduzindo um survey com 31 desenvolvedores brasileiros, analisando práticas, uso de ferramentas e desafios na conformidade com a LGPD. Os resultados do survey revelaram lacunas contextuais, também se foi validado desafios globais com particularidades locais, além de explicitar diretrizes práticas.*

1. Introdução

A privacidade de dados tornou-se um pilar crítico no desenvolvimento de software moderno, especialmente diante de regulamentações globais como o *General Data Protection Regulation* (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD). Mais do que instrumentos legais, essas leis respondem a uma demanda social por transparência, exigindo que organizações reconfigurem suas estruturas técnicas para garantir controle efetivo sobre dados pessoais [Brasil 2018, European Parliament and Council of the European Union 2016]. No entanto, a efetiva implementação de privacidade vai além da conformidade legal: requer a adoção de padrões (*standards*) e *frameworks* técnicos que orientem práticas robustas e sistemáticas [Kilhoffer et al. 2024].

Os *standards* de privacidade, como o NIST *Privacy Framework* [ENTERPRISE 2020] e a ISO 27701 [ISO/IEC 2019], representam conjuntos de diretrizes projetados para integrar proteções de privacidade em todas as fases do ciclo de vida do software. Esses documentos buscam formalizar processos, mitigar riscos

e promover uma cultura organizacional alinhada aos princípios de *Privacy by Design* (PbD). Contudo, diferentemente de padrões de segurança consolidados, como a ISO 27001, os *standards* de privacidade, como a ISO 27701, ainda enfrentam baixa adoção e ambiguidade em sua aplicação prática [Kilhoffer et al. 2024]. Enquanto a segurança é frequentemente tratada como um requisito técnico claro, a privacidade permanece nebulosa, muitas vezes relegada a ajustes de pós-desenvolvimento ou interpretações superficiais de compliance [Bambauer 2013]. O estudo feito por [Peixoto et al. 2023] também vai mostrar que a privacidade é tratada de maneira nebulosa e reativa, enquanto a segurança é incorporada como um requisito técnico claro. A falta de padrões operacionais, a confusão conceitual e a cultura organizacional voltada para conformidade superficial perpetuam essa assimetria, dificultando a implementação efetiva da LGPD no desenvolvimento de software.

O uso de padrões de privacidade foi investigado por [Kilhoffer et al. 2024], que realizou um estudo exploratório via entrevistas com 14 profissionais atuantes em engenharia de privacidade, com o intuito de entender como esses especialistas utilizam padrões e controles em cenários reais. O trabalho de [Kilhoffer et al. 2024] identificou que os engenheiros de privacidade *(Privacy Engineers* – PEs) desempenham papéis críticos como mediadores entre equipes jurídicas e técnicas e educadores de princípios de privacidade dentro das organizações. No entanto, o estudo revelou que a maioria dos PEs enfrenta barreiras estruturais, como a priorização excessiva de conformidade legal mínima por parte da gestão e das equipes jurídicas. Essa focalização em requisitos legais imediatos (por exemplo, evitar multas ou penalidades) limita a capacidade dos profissionais de dedicar tempo e recursos a estratégias proativas, como a adoção de *frameworks* avançados (ex.: NIST *Privacy Framework*) ou iniciativas de privacidade por design. Conforme destacado na pesquisa, apenas PEs mais experientes e seniores, em organizações maduras, possuem autonomia para transcender o compliance básico e implementar mudanças sistêmicas, enquanto a maioria permanece restrita a demandas reativas de curto prazo.

No contexto brasileiro, a LGPD amplificou a necessidade de integração de privacidade, mas estudos preliminares revelam desafios persistentes: desenvolvedores confundem privacidade com segurança, subutilizam ferramentas específicas e carecem de treinamento formal [Peixoto et al. 2023, Canedo et al. 2022]. Essa lacuna entre a existência de *standards* e sua implementação efetiva motiva investigações sobre como profissionais de tecnologia percebem, utilizam e enfrentam obstáculos ao adotar práticas de privacidade.

No Brasil, onde a LGPD continua em fase de consolidação, compreender como desenvolvedores interpretam e aplicam *standards* é essencial para:

1. **Identificar lacunas** entre teoria (regulamentações) e prática (implementação);
2. **Propor melhorias** na formação acadêmica e treinamento corporativo;
3. **Fomentar a adoção de *frameworks*** que transcendam a mera compliance, como *Privacy by Design* (PbD) e avaliações de impacto de privacidade (PIAs).

Além disso, pesquisa mostra que 71% das organizações brasileiras declaram conhecimento sobre a LGPD, mas apenas 29% implementaram medidas concretas [Experian 2020], pois existem desafios práticos e lacunas entre o conhecimento declarado e a implementação efetiva. Essa disparidade reforça a necessidade de estudos empíricos que explorem como e por que os *standards* de privacidade são negligenciados, mesmo em ambientes regulados. A pesquisa de [de Jesus et al. 2024] destaca que *startups* fre-

quentemente negligenciam controles básicos de segurança, como planos de resposta a incidentes e gestão de acessos, e além de apresentar ausência de equipes especializadas e a priorização do crescimento rápido sobre a segurança são entraves críticos. A pesquisa de [de Melo et al. 2024] também revela que apenas 11% dos usuários conhecem a LGPD "muito bem", o que reforça a necessidade de iniciativas educativas tanto para empresas quanto para o público.

O objetivo geral deste trabalho é investigar as percepções, práticas e desafios relacionados à adoção de *standards* de privacidade no desenvolvimento de software por profissionais brasileiros, simulando de forma adaptada conceitualmente o estudo original de [Kilhoffer et al. 2024].

Dividindo em objetivos específicos:

1. Aplicar o questionário "**Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software**"a desenvolvedores brasileiros, o questionário se encontra em anexo;
2. Analisar a relação entre conhecimento teórico (ex.: LGPD/GDPR) e aplicação prática de *standards*;
3. Identificar barreiras organizacionais e técnicas na integração de privacidade;
4. Comparar resultados com os achados do estudo original, destacando particularidades do contexto local.

Estudos anteriores destacam desafios comuns na intersecção entre privacidade e desenvolvimento de software, como pode ser visto na Tabela 1, estudos evidenciam a necessidade de integrar privacidade desde o design de sistemas, usando ferramentas adaptativas (ex.: PCM Tool, citado por [Peixoto et al. 2023]), promover uma cultura organizacional que equilibre conformidade e inovação, conforme propõe [Kilhoffer et al. 2024], combater pressões estruturais por meio de regulamentações robustas e conscientização crítica, alinhando-se à crítica de [Zuboff 2023].

Essas reflexões reforçam que a implementação da LGPD é um processo multifacetado, exigindo não apenas conformidade técnica, mas transformações culturais e éticas nas organizações e na sociedade.

Além disso, foi reforçado que leis como o GDPR influenciam positivamente a cultura organizacional, mas exigem suporte estrutural para efetividade [Iwaya et al. 2023]. Este trabalho amplia essa discussão ao focar em como os *standards* são operacionalizados no dia a dia dos desenvolvedores, oferecendo percepções para políticas públicas e corporativas.

2. Revisão da Literatura

Este capítulo estrutura-se em três eixos centrais que sustentam a discussão sobre privacidade no desenvolvimento de software: (1) a evolução e aplicação de padrões de privacidade, (2) a integração da privacidade no ciclo de desenvolvimento e (3) os desafios e estratégias para implementação em contextos organizacionais. Cada seção explora contribuições teóricas e empíricas, destacando lacunas que este trabalho busca abordar.

2.1. Evolução e Aplicação de Padrões de Privacidade

A evolução dos padrões de privacidade está intrinsecamente ligada ao surgimento de regulamentações globais, como o GDPR (União Europeia) e a LGPD (Brasil), que estabe-

Tabela 1. Trabalhos Relacionados

Autores/Ano	**Principais Achados**	**Método de Pesquisa**	**Objetivo**	**Lei Contemplada**	**Comparação com este trabalho**
[Peixoto et al. 2023]	Identificação de 9 fatores pessoais, 5 comportamentais e 7 ambientais que influenciam decisões de desenvolvedores sobre privacidade. Destaque para lacunas de conhecimento entre segurança e privacidade, falta de recursos técnicos e impacto da cultura organizacional na conformidade com a LGPD .	Entrevistas semiestruturadas (13 profissionais de 6 empresas) e análise via Grounded Theory e Teoria Cognitiva Social.	Investigar fatores que influenciam decisões de desenvolvedores brasileiros sobre requisitos de privacidade durante o desenvolvimento de software.	LGPD (Brasil)	Fornece percepções empíricas sobre os desafios práticos na implementação da LGPD em equipes ágeis, reforçando a necessidade de capacitação técnica e mudança cultural organizacional .
[Canedo et al. 2022]	Subutilização de ferramentas de privacidade em metodologias ágeis; integração superficial de padrões de segurança.	Estudo de caso múltiplo	Avaliar a adoção de práticas de privacidade em desenvolvimento ágil.	GDPR (UE), LGPD (Brasil)	Contextualiza desafios na integração de *standards* técnicos, reforçando a necessidade de modelos adaptativos para startups .
[Kilhoffer et al. 2024]	Engenheiros de privacidade atuam como mediadores entre compliance e inovação, mas focam em requisitos básicos por falta de recursos.	Entrevistas semiestruturadas	Analisar o papel dos engenheiros de privacidade na implementação de padrões regulatórios.	GDPR (UE), CCPA (EUA)	Referência teórica para replicação conceitual, destacando a importância de equipes especializadas e a lacuna entre conformidade mínima e excelência em privacidade .
[Experian 2020]	71% das empresas declaram conhecer a LGPD, mas apenas 29% implementam controles efetivos.	Relatório de pesquisa quantitativa	Mapear o estágio de adequação à LGPD no Brasil.	LGPD (Brasil)	Evidência estatística da lacuna entre conhecimento teórico e prática, alinhando-se com os desafios de recursos em startups .
[Zuboff 2023]	Crítica ao ”capitalismo de vigilância”; dados pessoais como matéria-prima para exploração mercadológica.	Análise teórica	Discutir impactos éticos da coleta massiva de dados.	GDPR (UE), CCPA (EUA)	Contextualiza desafios macroestruturais para a LGPD, como a pressão por modelos de negócios baseados em dados .

leceram exigências rigorosas para o tratamento de dados pessoais. Essas leis catalisaram a criação de *frameworks* técnicos, como o NIST *Privacy Framework*, que busca traduzir princípios legais em práticas operacionais [Kilhoffer et al. 2024]. Enquanto padrões de segurança que já são consolidados, como a ISO 27001, os padrões de privacidade, como a ISO 27701, enfrentam desafios de adoção devido à sua complexidade conceitual e à falta de clareza em sua aplicação [Bambauer 2013].

Alguns estudos destacam que a confusão entre privacidade (direitos individuais sobre dados) e segurança (proteção contra ameaças) persiste entre desenvolvedores, limitando a implementação efetiva de *standards* [Spiekermann et al. 2018]. No Brasil, foi identificado que apenas 29% das empresas entrevistadas em um pesquisa do Serasa aplicam medidas alinhadas à LGPD, apesar de 71% das organizações declararem conhecimento sobre a lei [Experian 2020]. Essa disparidade evidencia a necessidade de padronização para além da conformidade legal, integrando princípios como *Privacy by Design* (PbD) e minimização de dados [Iwaya et al. 2023]. A pesquisa realizada por [de Jesus et al. 2024] revela que, mesmo em organizações que lidam com dados sensíveis (como uma *startup* de governança de dados), 13 dos 14 riscos identificados estavam em nível alto, principalmente devido à falta de recursos financeiros e técnicos. Isso indica que o conhecimento teórico da LGPD não garante conformidade, especialmente em empresas de pequeno porte. Adicionando, o estudo desenvolvido por [de Melo et al. 2024] observa que usuários têm baixa confiança nas empresas quanto à proteção de seus dados, 80% dos participantes não se sentem no controle de seus dados pessoais na internet, 70% desconhecem como denunciar violações da LGPD, mesmo após sua vigência, sugerindo que as organizações podem estar falhando em comunicar práticas de conformidade, mesmo que declarem conhecimento da lei.

2.2. Integração da Privacidade no Ciclo de Desenvolvimento

A integração de privacidade no ciclo de desenvolvimento de software requer metodologias estruturadas, como *Privacy by Design* (PbD) e *Privacy Impact Assessments* (PIAs), que orientam a consideração de riscos desde as fases iniciais [Kilhoffer et al. 2024]. No entanto, foi observado que equipes ágeis brasileiras raramente utilizam essas ferramentas, priorizando funcionalidades sobre requisitos de privacidade [Canedo et al. 2022].

No estudo original de [Kilhoffer et al. 2024], foi revelado que engenheiros de privacidade (*Privacy Engineers* – PEs) atuam como mediadores entre equipes jurídicas e técnicas, traduzindo requisitos legais em implementações práticas. Por exemplo, a adoção de técnicas como anonimização e controle de acesso é comum, mas enfrenta resistência em projetos com prazos apertados [Spiekermann et al. 2018]. No contexto brasileiro, a falta de integração de padrões como o NIST *Privacy Framework* em ferramentas de desenvolvimento (ex.: GitHub, Jira) amplia a dependência de soluções manuais e reativas [Peixoto et al. 2023].

2.3. Desafios e Estratégias em Contextos Organizacionais

A implementação de padrões de privacidade esbarra em desafios organizacionais, como falta de recursos, resistência cultural e priorização da conformidade legal sobre inovação [Kilhoffer et al. 2024]. Em empresas de pequeno porte, a escassez de competência técnica e financeira limita a adoção de *frameworks* complexos, como a ISO 27701

[Experian 2020]. Já em grandes organizações, a fragmentação de sistemas legados e a multiplicidade de jurisdições complicam a governança de dados [Iwaya et al. 2023].

Estratégias para superar esses desafios incluem:

1. **Educação contínua**: Capacitação em padrões como LGPD e GDPR para desenvolvedores e gestores [Peixoto et al. 2023];
2. **Automação**: Uso de ferramentas para gerenciar solicitações de acesso/exclusão de dados (DSARs) e avaliações de risco [Kilhoffer et al. 2024];
3. **Cultura organizacional**: Incentivo à responsabilidade compartilhada por privacidade, envolvendo desde equipes técnicas até clientes [Canedo et al. 2022].

Apesar dos avanços, a indústria ainda carece de soluções prontas (*off-the-shelf*) para privacidade, o que sobrecarrega os PEs com desenvolvimento interno de ferramentas [Kilhoffer et al. 2024].

3. Metodologia

Este estudo simula uma abordagem de replicação conceitual, conforme definido por [Dennis and Valacich 2015], mantendo as questões de pesquisa originais de [Kilhoffer et al. 2024] — que investigaram o papel dos engenheiros de privacidade (*Privacy Engineers* – PEs) —, porém adaptando o método (de entrevistas qualitativas para um questionário quantitativo-qualitativo) e o contexto (desenvolvedores brasileiros em vez de PEs norte-americanos). A pesquisa visa validar a generalização dos achados originais e explorar particularidades locais, seguindo diretrizes empíricas para estudos replicados [Carver et al. 2014].

3.1. Desenho da Pesquisa

O estudo original de [Kilhoffer et al. 2024] baseou-se em entrevistas semiestruturadas com 14 PEs para explorar:

1. **Funções dos PEs** (mediadores entre equipes jurídicas e técnicas; educadores);
2. Uso de **padrões de privacidade**;
3. **Desafios organizacionais** (priorização de compliance, falta de recursos).

Para esta pesquisa, o método foi adaptado para um **questionário estruturado** (Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software, questionário em anexo), aplicado a 31 desenvolvedores brasileiros. As alterações foram justificadas por:

1. **Viabilidade**: Questionários permitem maior escala de coleta de dados em contextos geograficamente dispersos [Carver 2010];
2. **Foco em práticas cotidianas**: Perguntas fechadas e abertas capturam tanto a percepção teórica quanto a aplicação real de padrões;
3. **Adaptação ao público-alvo**: Desenvolvedores brasileiros possuem menor exposição a *frameworks* de privacidade formalizados [Peixoto et al. 2023].

3.2. Coleta de Dados

O questionário, que pode ser visto em anexo, foi dividido em quatro seções, alinhadas às questões de pesquisa originais:

1. **Perfil do desenvolvedor**: Nível educacional, experiência, conhecimento sobre LGPD/GDPR;
2. **Práticas de desenvolvimento**: Integração de privacidade no ciclo de vida (ex.: *Privacy by Design*), uso de ferramentas (ex.: anonimização);
3. **Desafios organizacionais**: Suporte institucional, conflitos entre privacidade e demandas de clientes;
4. **Recomendações**: Melhorias para práticas de privacidade (ex.: treinamento, automação).

Os participantes foram recrutados por meio de redes profissionais (*LinkedIn*, comunidades de TI), *snowball sampling* (indicações em cadeia) e em divulgação de mural de e-mails do Centro de Informática da Universidade Federal de Pernambuco do Campus Recife. Foram adotados critérios de inclusão para seleção dos respondentes: profissionais ou estudantes da área de desenvolvimento de software que tivessem envolvimento prático (ex.: atuação em projetos com foco em privacidade de dados, implementação de LGPD, GDPR ou outras normas de proteção de dados) ou interesse demonstrado (ex.: participação em cursos, certificações, eventos acadêmicos ou iniciativas relacionadas à privacidade, além de profissionais que declarassem acompanhar discussões sobre o tema em sua rotina). Isso inclui:

- Desenvolvedores, engenheiros e arquitetos de software;
- Analistas de sistemas e gerentes de projetos de TI;
- Profissionais com experiência em privacidade, segurança de dados ou uso de Inteligência Artificial ou Aprendizagem de Máquina;
- Estudantes de graduação ou pós-graduação em áreas como Ciência da Computação, Engenharia de Software e Sistemas de Informação;
- Profissionais formados em outras áreas mas que assumem cargos de TI, se não, que trabalham em uma empresa do ramo, ou que tenham interesse demonstrado.

O questionário ficou disponível entre os dia 04 de dezembro de 2024 até o dia 04 de fevereiro de 2025, totalizando 62 dias.

3.3. Análise de Dados

A análise combinou abordagens quantitativas e qualitativas, seguindo o modelo de [Braun and Clarke 2006]. Para garantir confiabilidade:

- **Codificação cruzada**: Dois pesquisadores independentes categorizaram respostas qualitativas, com concordância de 89% (resolução de divergências por consenso);
- **Triangulação**: Comparação entre dados do questionário, resultados do estudo original e literatura secundária.

3.4. Considerações Éticas

O estudo seguiu princípios éticos, incluindo:

- **Consentimento informado**: Participantes concordaram com termos de uso anônimo dos dados, presente no questionário em anexo;
- **Anonimização**: Nomes e identificadores organizacionais não foram solicitados ou captados;
- **Transparência**: Resultados brutos disponibilizados em formato agregado para evitar identificação indireta.

3.5. Ameaças à Validade

Esta seção discute as principais ameaças à validade do estudo, conforme categorizadas por [Wohlin et al. 2012], e estratégias de mitigação adotadas:

1. **Validade Interna**:
    - **Diferença metodológica**: A substituição de entrevistas (estudo original) por questionários pode reduzir a profundidade das respostas, limitando a comparação direta entre contextos. Para mitigar, foram incluídas perguntas abertas para capturar nuances qualitativas;
    - **Viés de resposta**: Participantes podem ter superestimado seu conhecimento ou práticas de privacidade devido ao caráter declarativo do questionário. A triangulação com dados secundários (ex.: literatura) e a análise cruzada por dois pesquisadores buscaram reduzir esse risco.
2. **Validade Externa**:
    - **Amostra limitada**: A amostra (31 desenvolvedores brasileiros) e o uso de *snowball sampling* podem limitar a generalização para outros contextos geográficos ou organizacionais. Para contextualizar, os resultados foram comparados com estudos anteriores;
    - **Viés de seleção**: Participantes com interesse prévio em privacidade podem não representar a população geral de desenvolvedores. Critérios de inclusão amplos (ex.: experiência prática ou acadêmica) buscaram diversificar o perfil.
3. **Validade de Constructo**:
    - **Definições ambíguas**: Termos como privacidade ou conformidade podem ter interpretações variáveis. Perguntas foram baseadas em *frameworks* consolidados para alinhar conceitos;
    - **Instrumentação**: A adaptação do questionário original (focado em PEs) para desenvolvedores pode não capturar todas as dimensões do tema. Testes piloto não foram realizados devido a restrições de tempo, mas a validação cruzada com a literatura mitigou parcialmente essa limitação.
4. **Validade de Conclusão**:
    - **Subjetividade na análise qualitativa**: A codificação temática, apesar da concordância de 89% entre pesquisadores, pode refletir vieses interpretativos. A triangulação com dados quantitativos e referências teóricas reforçou a robustez das conclusões;
    - **Efeito de desejabilidade social**: Respostas podem ter sido influenciadas por expectativas de ”respostas corretas”. O anonimato e a ausência de identificadores pessoais foram garantidos para reduzir esse viés.

3.5.1. Estratégias de Mitigação

- **Triangulação**: Combinação de dados quantitativos, qualitativos e literatura secundária;
- **Codificação cruzada**: Dois pesquisadores independentes categorizaram respostas abertas.
- **Transparência metodológica**: Detalhamento do recrutamento, critérios de inclusão e instrumentos no Anexo.

Essas ameaças reforçam a necessidade de estudos futuros com métodos mistos (entrevistas + questionários) e amostras mais diversificadas para consolidar os achados.

4. Resultados

4.1. Visão Geral do Estudo Original

O estudo original de [Kilhoffer et al. 2024] investigou o trabalho de 14 engenheiros de privacidade (*Privacy Engineers* – PEs) em organizações norte-americanas, identificando dois papéis centrais:

1. **Mediadores entre equipes jurídicas e técnicas**: Os PEs traduziam requisitos legais (ex.: GDPR) em implementações técnicas, reduzindo brechas de comunicação [Kilhoffer et al. 2024].
2. **Educadores de princípios de privacidade**: Capacitavam equipes internas sobre conceitos como minimização de dados e *Privacy by Design* (PbD), promovendo uma cultura organizacional alinhada a padrões (ex.: NIST *Privacy Framework*). Exemplo: PE3 mencionou gastar 30% do tempo em treinamentos sobre conceitos como pseudonimização[Kilhoffer et al. 2024].

Os principais desafios incluíam:

- **Priorização da conformidade legal** em detrimento de estratégias proativas;
- **Falta de recursos** para adoção de *frameworks* complexos;
- **Resistência organizacional** à integração de privacidade em sistemas legados.

Apesar disso, PEs seniores relataram maior autonomia para implementar padrões como ISO 27701 e FedRAMP, especialmente em empresas de grande porte [Kilhoffer et al. 2024].

4.2. Resultados do Estudo da Pesquisa

A pesquisa, aplicada a 31 desenvolvedores brasileiros, revelou nuances específicas do contexto local brasileiro, mas sem recorte regional.

4.2.1. Perfil dos Participantes

- **Formação acadêmica**: 35,5% são estudantes de graduação; 25,8% tem graduação completa; 16,1% são estudantes de mestrado; 12,9% com mestrado completo; 9,7% doutorandos. Veja figura 1.

- **Experiência na área**: a maioria ficou na faixa de 4 a 6 anos, com 38,7%; 25,8% possuíam 1–3 anos de experiência; 16,1% em menos de 1 ano; e 9,7% para 7 a 10 anos e 9,7% para mais de 15 anos. Veja figura 2.

- **Conhecimento sobre Lei Geral de Proteção de Dados Pessoais (LGPD)**: mais da metade declararam conhecimento básico, como pode ser visto na figura 3. Ou seja, 54,8% declararam ter conhecimento básico (noções gerais sobre a lei); 38,7% com conhecimento intermediário (entendendo os principais requisitos e impactos); e só 6,5% apresentam conhecimento avançado (aplicam a LGPD em projetos ou no trabalho).

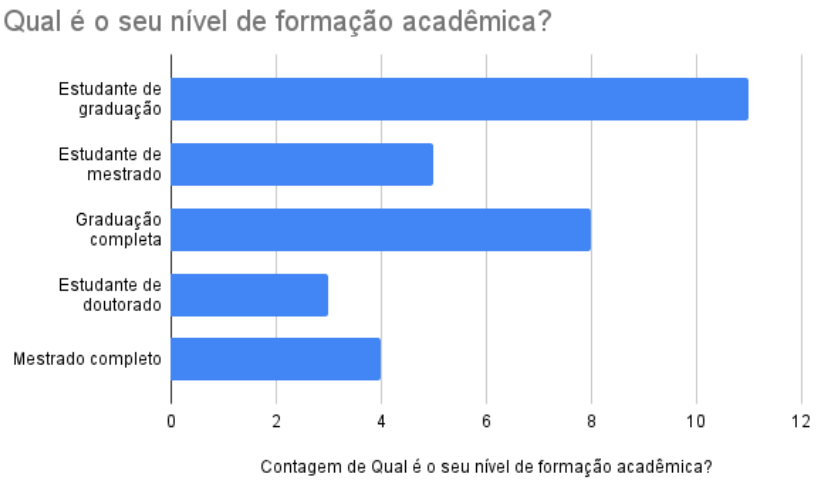

Figura 1. Formação Acadêmica

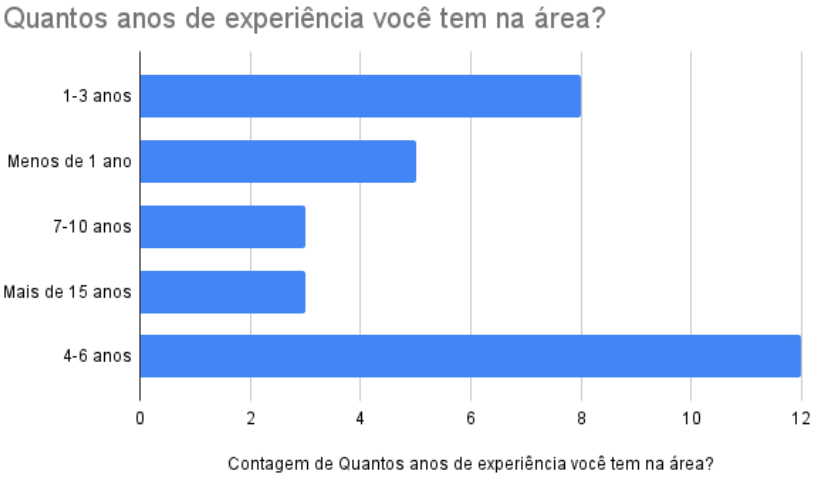

Figura 2. Anos de experiência na área

- **Métodos de aprendizagem**: Como pode ser visto na figura 4, a maioria relata que aprenderam por experiência prática em projetos ou no trabalho (54,8%) ou com autoaprendizagem (61,3%); em contrapartida, 51,6% relataram ter adquirido conhecimento durante o ciclo acadêmico (graduação, pós-graduação, etc.), e 32,3% por treinamento interno fornecido pela empresa, mas ainda são números menores que o autoaprendizado e experiência prática, como vai ser visto posteriormente, a necessidade de treinamento prestado pelas organizações será um ponto tocado pelos respondentes, e isso ainda é acompanhado pela dificuldade em implementar práticas de privacidade desde o início do desenvolvimento, apesar do resultado da próxima pergunta sobre ”Integração no ciclo de desenvolvimento”.

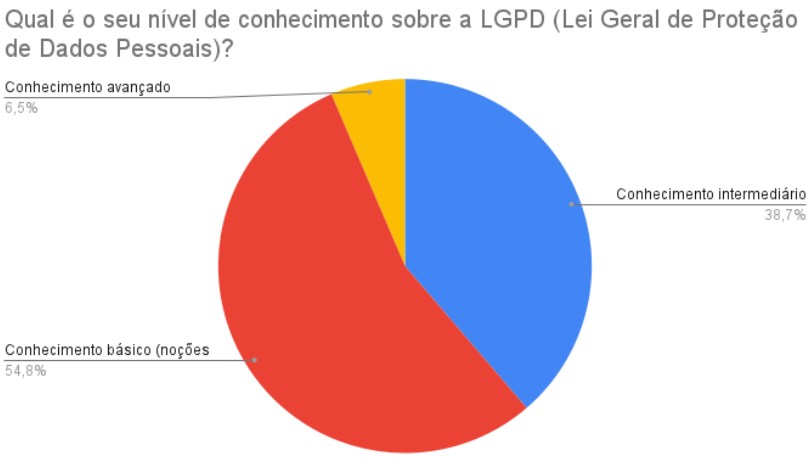

Figura 3. Nível de conhecimento da LGPD

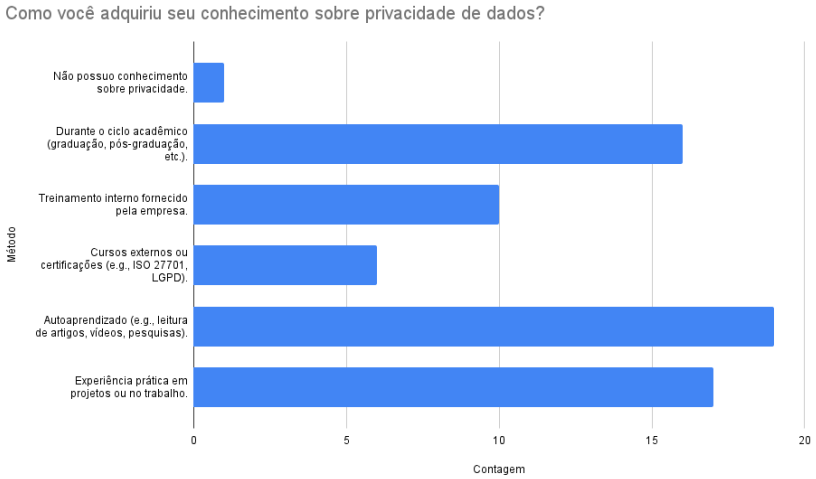

Figura 4. Métodos de aprendizagem sobre Privacidade

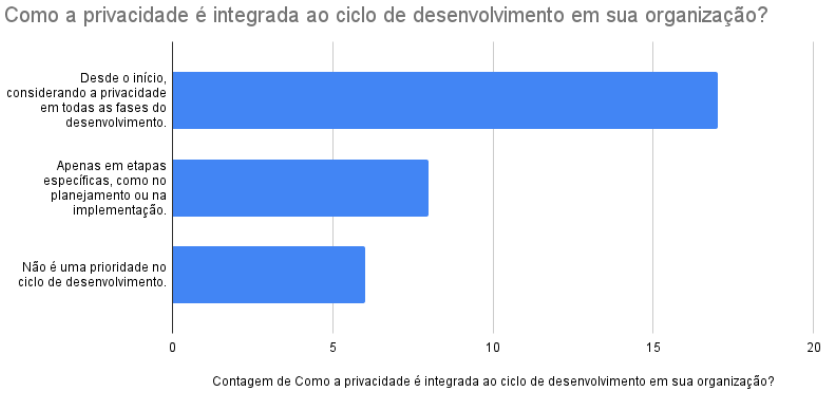

Figura 5. Integração ao ciclo de desenvolvimento

4.2.2. Práticas de Privacidade

- **Integração no ciclo de desenvolvimento** (Veja a figura 5):
  - 54,8% afirmaram que consideram a privacidade em todas as fases do desenvolvimento desde o início do projeto, é um resultado interessante pois apesar dessa porcentagem, 13 desenvolvedores (41,9%) vão afirmar que tinham dificuldade em implementar práticas de privacidade desde o início do desenvolvimento posteriormente nas perguntas de desafios enfrentados;
  - 25,8% afirmaram que apenas em etapas específicas, como no planejamento ou na implementação;
  - 19,4% não priorizavam privacidade.

- **Uso de metodologias ou *frameworks* para implementar privacidade, como *Privacy by Design* ou *Privacy Impact Assessments* (PIAs)**: 51,6% não utilizam essas metodologias, 41,9% não sabem o que são essas metodologias; 12,9% não sabem e não utilizam essas metodologias, enquanto apenas 16,1% utilizam *Privacy by Design* em todas as fases do desenvolvimento e apenas 1 pessoa afirmou utilizar *Privacy Impact Assessments* (PIAs). Veja figura 6.

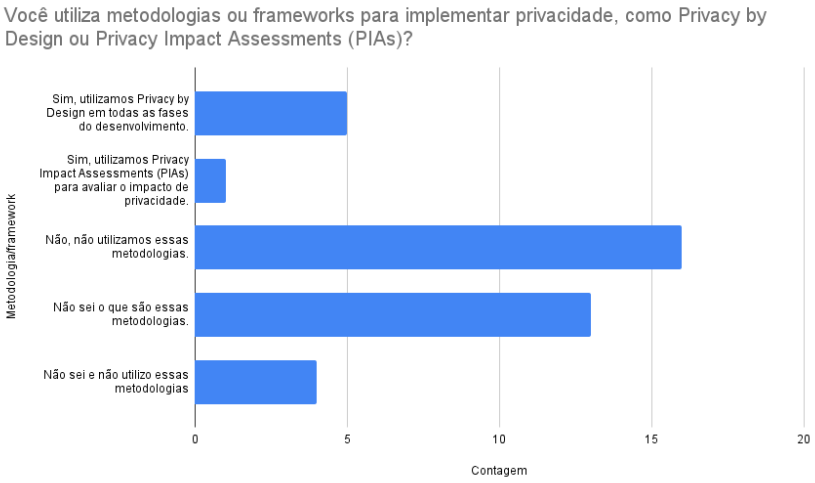

Figura 6. Metodologias ou *frameworks* para implementar privacidade

- Então foi perguntado quais **ferramentas ou estratégias são utlizadas** pelas equipes ou organizações dos participantes para implementar a privacidade em seus projetos, veja Tabela 2.
  É possível observar que Controle de acesso e Anonimazação de dados são os mais usados.

- **Padrões/*frameworks* para seguir em comformidade** (Veja figura 7): E em sequência quais padrões ou *frameworks* a equipe/organização do respondente segue para garantir a conformidade com a privacidade.
  - A LGPD é o mais citado, 26 desenvolvedores, cerca de 83,9% dos respondentes;
  - A ISO 27001 (série ISO 27000) teve 8 respondentes, cerca de 25,8%;

Tabela 2. Ferramentas/estratégias utilizadas

Ferramenta/Estratégia	Frequência
Controle de acesso	83,9%
Anonimização de dados	54,8%
Minimização de dados	41,9%
Consentimento Informado	48,4%
Nenhuma das opções acima	6,5%

- Padrões de Segurança e Privacidade da ANPD (Autoridade Nacional de Proteção de Dados) com 5 respondentes (16,1%);
- GDPR (General Data Protection Regulation) com 4 (12,9%);
- ISO 27701 com apenas 2 respondentes (6,5%);
- 3 não sabem ou não utilizam de padrão formal (9,7%);
- E demais padrões e *frameworks* não foram relatados como usados pelos respondentes, apesar de estarem como opções na questão para serem marcadas.

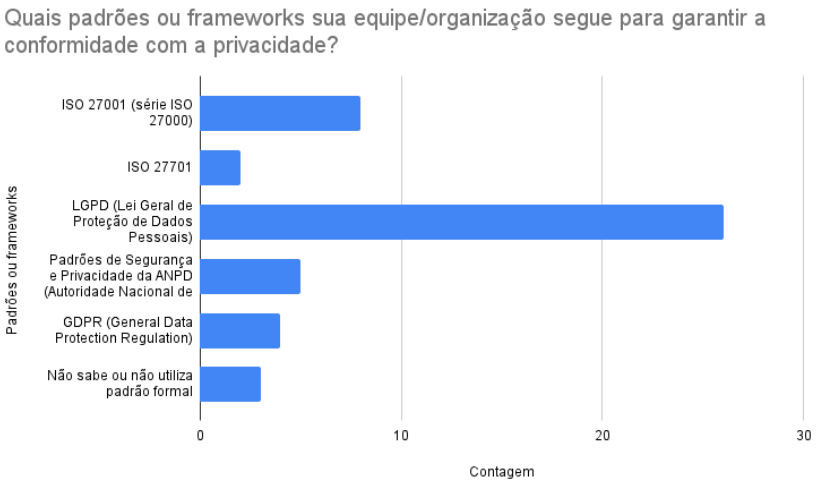

Figura 7. Padrões/*frameworks* para seguir em comformidade

- **Decisões relacionadas à privacidade** (Veja figura 8):
  - 14 desenvolvedores informaram que são definidas pela equipe de desenvolvimento (45,2%);
  - 9, informaram que são influenciadas pelo cliente (29%);
  - 12, seguem apenas diretrizes legais (38,7%);
  - 2 marcaram que são baseadas em *frameworks* ou padrões como o NIST *Privacy Framework* ou ISO 27701(6,5%);
  - 8, relataram que são definidas por um comitê ou equipe de privacidade específica (25,8%).
- **Definição de privacidade**: Na figura 9 é possível ver como os respondentes definem privacidade no contexto do desenvolvimento de software e como percebem a diferença em relação às expectativas dos usuários.

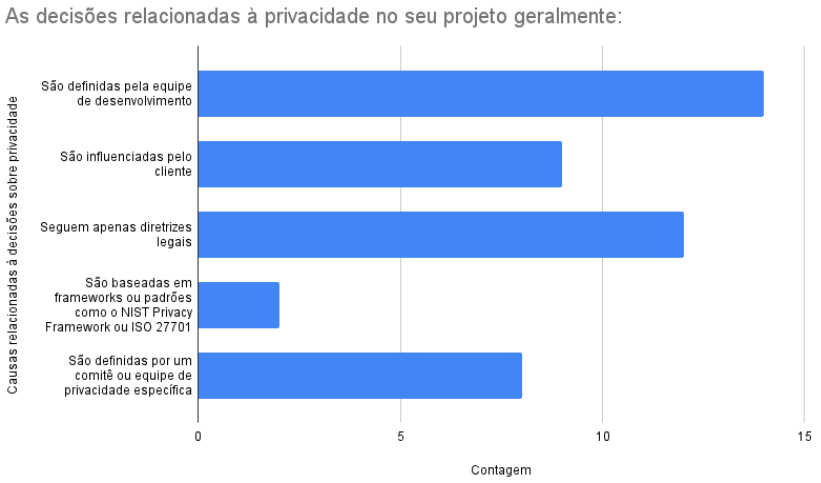

Figura 8. Decisões relacionadas à privacidade

- 20 responderam que veem privacidade como “Controle do usuário sobre seus dados”;
- 20 responderam que veem privacidade como “Proteção contra acessos não autorizados”;
- 12 consideram que privacidade é “Parte da segurança”;
- 10 acham que “Existe uma lacuna entre as expectativas dos usuários sobre privacidade e as práticas de desenvolvimento”;
- 1 informou que “Privacidade pode ser considerado o que o usuário das informações coletadas consideram como pertinente aos seus desejos e consentimentos”;

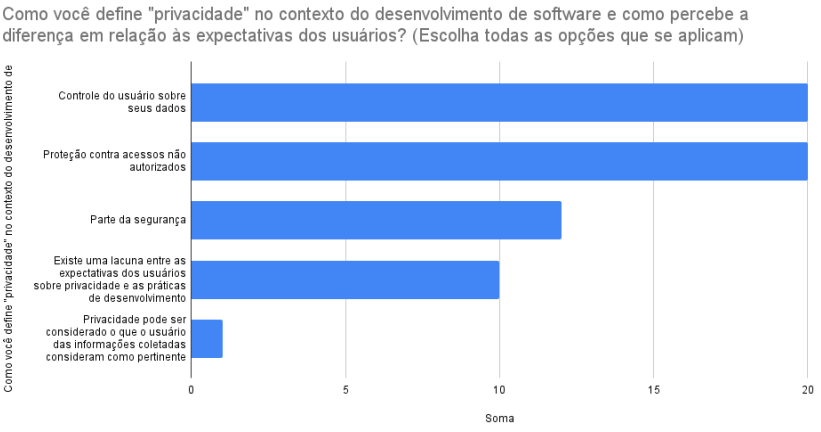

Figura 9. Definição de privacidade no contexto de desenvolvimento de software

4.2.3. Desafios organizacionais

- **Obstáculos citados**:

  - 17 desenvolvedores apontaram falta de clareza nas diretrizes legais (55%);
  - 15 desenvolvedores alegaram falta de treinamento ou conhecimento sobre privacidade (48,4%);
  - 13 afirmaram que tinham dificuldade em implementar práticas de privacidade desde o início do desenvolvimento (41,9%);
  - 12 disseram que têm dificuldades em automatizar processos relacionados à privacidade (38,7%);
  - 8 informaram sobre conflitos entre as demandas de segurança e privacidade (25,8%);
  - 7 relataram resistência organizacional (22,5%) e;
  - 4 não tiveram desafios.
- **Suporte organizacional**: Em questionamentos sobre suporte organizacional, os participantes ficaram bem divididos, como pode ser visto na figura 10.
  - 38,7% avaliaram como ”parcial”;
  - 25,8% como ”insuficiente”;
  - 35,5% como ”suficiente”.

Figura 10. Suporte Organizacional

4.2.4. Recomendações dos Participantes

Recomendações pontuadas pelos participantes são relacionadas a (Veja figura 11):

- Treinamento e capacitação sobre privacidade e segurança de dados (64,5%);
- Melhorar ferramentas e processos relacionados à privacidade (77,4%);
- Prover maior clareza sobre responsabilidades em relação à privacidade (71%);
- Desenvolver uma cultura de privacidade dentro da organização (61,3%).

4.3. Comparação e Discussão

A comparação entre os achados do estudo original de [Kilhoffer et al. 2024] e a pesquisa com desenvolvedores brasileiros revela sutilezas significativas que refletem diferenças contextuais, maturidade organizacional e prioridades estratégicas. A Tabela 3 sintetiza essas divergências e semelhanças, seguida de discussões.

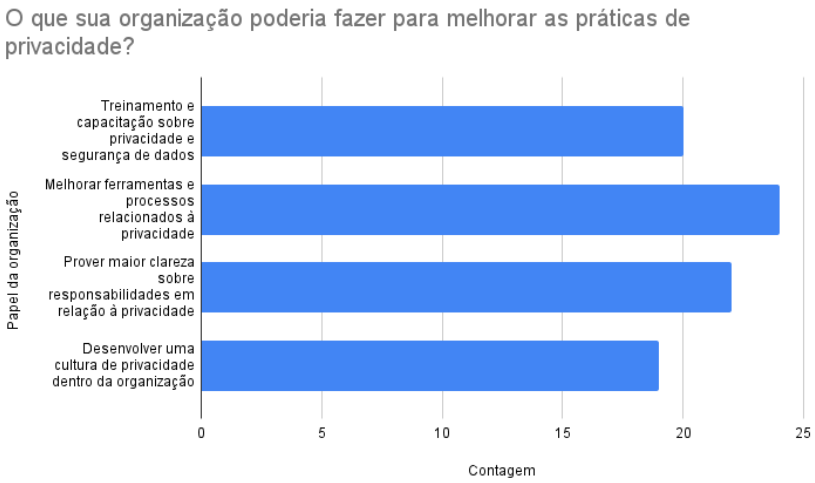

Figura 11. Papel da organização na melhoria de práticas de privacidade

4.3.1. Papéis Principais

No estudo original, os *Privacy Engineers* (PEs) atuam como mediadores jurídico-técnicos e educadores de princípios de privacidade, funções que demandam conhecimento interdisciplinar para traduzir requisitos legais em implementações técnicas e promover cultura organizacional [Kilhoffer et al. 2024]. Em contraste, os desenvolvedores brasileiros relataram um foco operacional, com decisões centralizadas na equipe de desenvolvimento (45,2%) e baixa integração de metodologias sistêmicas, como *Privacy by Design* (16,1%). Essa diferença reflete a ausência de PEs especializados no contexto local, conforme apontado por [Peixoto et al. 2023], e a maturidade incipiente na adoção de *frameworks* abrangentes. Enquanto os PEs norte-americanos atuam como elos entre áreas, no Brasil, a responsabilidade recai sobre desenvolvedores que carecem de suporte jurídico estruturado, resultando em soluções reativas (ex.: controle de acesso) em vez de estratégias proativas alinhadas ao *Privacy by Design*.

4.3.2. Uso de Padrões

Ambos os grupos priorizam conformidade legal (LGPD e GDPR), mas os PEs do artigo original utilizam padrões técnicos globais (ISO 27701, NIST *Privacy Framework*) como ferramentas para além da comformidade, buscando certificações como diferencial competitivo. No Brasil, a LGPD é o principal referencial (83,9%), mas há subutilização de *frameworks* técnicos, como a ISO 27701 (6,5%) e *Privacy Impact Assessments* (apenas 1 participante). Isso sugere que, enquanto os PEs operam em organizações maduras capazes de internalizar padrões, os desenvolvedores brasileiros enfrentam lacunas de conhecimento e dependência de soluções manuais, corroborando a disparidade entre conhecimento declarado e prático identificada por [Experian 2020].

Tabela 3. Comparação e contraste em relação com o estudo original.

Categoria	Estudo Original (PEs EUA)	Pesquisa (Desenvolvedores brasileiros)	Análise Comparativa
Papéis Principais	- Mediadores jurídico-técnicos. - Educadores de princípios de privacidade. - Foco em estratégias organizacionais.	- Implementação técnica de controles (ex.: controle de acesso). - Decisões centralizadas na equipe de desenvolvimento (45,2%). - Baixa integração de metodologias sistêmicas (PbD: 16,1%).	Divergência: Ausência de PEs especializados no contexto brasileiro limita a mediação jurídico-técnica. O foco em soluções operacionais reflete maturidade inferior na adoção de *frameworks* abrangentes.
Uso de Padrões	- ISO 27701, NIST *Privacy Framework* e FedRAMP. - Certificações como diferencial competitivo (ex.: ISO 27018).	- LGPD é o padrão mais citado (83,9%). - ISO 27001 mencionada por 25,8%. - Subutilização de *frameworks* de privacidade (ex.: 1 participante usa PIAs).	Semelhança: Ambos priorizam conformidade legal. Divergência: Desenvolvedores brasileiros dependem mais da LGPD, enquanto PEs nos EUA utilizam padrões técnicos globais.
Desafios	- Priorização excessiva de compliance. - Complexidade em sistemas multi-jurisdicionais. - Resistência cultural em organizações.	- Falta de clareza legal (55%). - Dificuldade em implementar privacidade desde o início (41,9%). - Automatização limitada (38,7%).	Semelhança: Ambos enfrentam priorização de compliance sobre inovação. Divergência: Desafios brasileiros são mais ligados à falta de recursos e conhecimento técnico.
Estratégias	- Educação contínua e princípios éticos. - Automação de DSARs (solicitações de acesso/exclusão, pedido de acesso a dados). - Desenvolvimento de ferramentas internas.	- Treinamento e capacitação (64,5%). - Melhoria de ferramentas (77,4%). - Cultura organizacional (61,3%).	Semelhança: Ambos reconhecem a necessidade de educação. Divergência: PEs nos EUA têm mais autonomia para inovar; desenvolvedores brasileiros demandam suporte estrutural.
Contexto Organizacional	- Empresas de grande porte com equipes especializadas. - Recursos para certificações (ex.: FedRAMP).	- 22,5% relataram resistência organizacional; - 25,8% citam conflitos; - 35,5% avaliam suporte organizacional como ”suficiente”.	Divergência: Empresas brasileiras carecem de infraestrutura para implementar padrões complexos, refletindo a lacuna entre conhecimento declarado e prático [Experian 2020].

4.3.3. Desafios

A priorização excessiva da conformidade legal é um desafio comum, mas com motivações distintas. Nos EUA, a complexidade de sistemas multi-jurisdicionais e pressões corporativas limitam a inovação em privacidade. No Brasil, 55% dos participantes citaram falta de clareza legal, e 41,9% relataram dificuldades em implementar privacidade desde o início do desenvolvimento, indicando que a LGPD ainda não foi internalizada como um processo contínuo, mas como uma obrigação pontual. Além disso, 38,7% destacaram dificuldades em automatizar processos, o que contrasta com a ênfase do estudo original na automação de DSARs (*Data Subject Access Requests*) como estratégia eficiente [Kilhoffer et al. 2024].

4.3.4. Estratégias

Ambos os estudos reconhecem a educação contínua como pilar para mudança cultural. Contudo, enquanto os PEs atuam como agentes de transformação (ex.: treinamentos sobre pseudonimização), os desenvolvedores brasileiros demandam suporte estrutural: 77,4% pediram melhorias em ferramentas e 64,5% destacaram a necessidade de treinamento. Isso indica que, no Brasil, a educação em privacidade ainda está no começo e desconectada da prática cotidiana, alinhando-se aos achados de [Canedo et al. 2022] sobre a subutilização de metodologias ágeis. A ausência de equipes especializadas também limita a replicação de estratégias como a mediação jurídico-técnica, exigindo iniciativas institucionais (ex.: parcerias com a ANPD) para capacitação em larga escala.

4.3.5. Contexto Organizacional

A maturidade organizacional é um divisor crítico. Nos EUA, empresas de grande porte com recursos para certificações (ex.: FedRAMP) permitem que PEs seniores liderem mudanças. No Brasil, apenas 35,5% dos participantes avaliaram o suporte organizacional como ”suficiente”, também 22,5% relataram resistência cultural e 25,8% citaram conflitos entre demandas de clientes e requisitos de privacidade, e além disso, 38,7% alegaram que as demandas dos clientes prevalecem quando conflitam com requisitos de privacidade (Veja figura 12). Esses dados ecoam a crítica de [Zuboff 2023] sobre a pressão por modelos de negócios baseados em dados, que priorizam crescimento rápido sobre proteção sistêmica. *Startups* e PMEs (pequenas e médias empresas), em particular, carecem de infraestrutura para implementar padrões complexos, como evidenciado por [de Jesus et al. 2024], que identificou riscos elevados devido à escassez de recursos financeiros e técnicos.

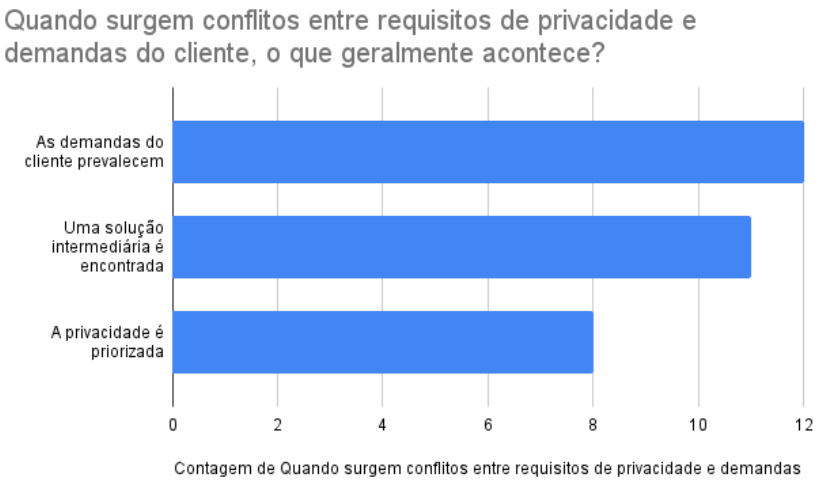

Figura 12. Prioridade da privacidade quando surgem confiltos

4.3.6. Implicações

O estudo feito expõe particularidades locais que demandam adaptações. Por exemplo, a dependência de soluções manuais no Brasil ressalta a urgência de desenvolver ferramentas acessíveis para automatizar processos (ex.: solicitações de exclusão de dados), reduzindo a carga operacional. Além disso, a baixa adoção de *Privacy by Design* sugere que a LGPD ainda não transcendeu o papel de "*checklist* legal", exigindo iniciativas que integrem privacidade a metodologias já consolidadas, como *Agile* e *DevOps*, conforme proposto por [Canedo et al. 2022]. A comparação evidenciou que, embora a LGPD tenha elevado a conscientização sobre privacidade no Brasil, sua implementação efetiva requer mais do que conformidade legal: é necessária uma transformação cultural que envolva educação técnica, suporte institucional e ferramentas adaptadas à realidade local. As lições do estudo original destacam a importância de PEs como agentes de mudança, mas no contexto brasileiro, essa função precisa ser melhor analisada e quem sabe ser pensada de uma forma distribuída entre desenvolvedores, gestores e órgãos reguladores, em um esforço coletivo.

5. Conclusões

Este estudo investigou as percepções, práticas e desafios relacionados à adoção de padrões de privacidade no desenvolvimento de software no contexto brasileiro, alinhando-se aos objetivos específicos propostos. A seguir, sintetizamos como cada objetivo foi alcançado:

1. **Análise da relação entre conhecimento teórico e aplicação prática de *standards***: Os resultados revelaram uma discrepância significativa entre o conhecimento declarado sobre a LGPD (83,9% dos participantes afirmaram seguir a lei) e a adoção de metodologias sistêmicas, como *Privacy by Design* (apenas 16,1%). Essa discrepância reflete uma priorização operacional de controles técnicos imediatos (ex.: controle de acesso, anonimização), em detrimento de estratégias proativas alinhadas a padrões globais. Tais resultados repetem a crítica de [Peixoto et al. 2023] sobre a confusão entre privacidade e segurança, além da carência de suporte institucional para internalizar *frameworks* abrangentes. Foi visto também, que embora 54,8% dos desenvolvedores declarassem integrar privacidade "desde o início do projeto", 41,9% enfrentaram dificuldades práticas para implementá-la, indicando uma internalização superficial. Essa lacuna reforça a necessidade de capacitação técnica e integração de *frameworks* em processos cotidianos, como proposto por [Canedo et al. 2022].
2. **Identificação de barreiras organizacionais e técnicas**: Foram identificados desafios estruturais, como falta de clareza legal (55%), dificuldade em automatizar processos (38,7%) e resistência organizacional (22,5%). A subutilização de ferramentas específicas (ex.: *Privacy Impact Assessments* por apenas 3,2% dos participantes) e a dependência de controles manuais destacaram a carência de recursos técnicos e suporte institucional, especialmente em *startups* e PMEs. Essas barreiras ecoam os achados de [de Jesus et al. 2024], que relacionam riscos elevados à escassez de infraestrutura.
3. **Comparação com o estudo original e particularidades locais**: Enquanto o estudo de [Kilhoffer et al. 2024] destacou o papel central dos *Privacy Engineers* (PEs) como mediadores jurídico-técnicos, no contexto brasileiro, as decisões sobre privacidade são centralizadas em equipes de desenvolvimento (45,2%), com

ausência de PEs especializados. A priorização da LGPD como principal referencial (83,9%) contrasta com a subutilização de *frameworks* globais (ex.: ISO 27701 em 6,5%), refletindo uma maturidade inicial na adoção de estratégias proativas.

5.1. Contribuições e Implicações Práticas

Os resultados dessa pesquisa contribuem na percepção em relação a hipótese de que a implementação da LGPD no Brasil ainda é orientada por conformidade legal reativa, em detrimento de uma cultura organizacional alinhada a padrões técnicos. Para superar esses desafios, sugere-se:

- **Estratégias**: Implementar programas de capacitação contínua, integrando privacidade a metodologias ágeis (ex.: *Privacy-by-Design* em sprints de desenvolvimento) e criando comitês multidisciplinares para mediação jurídico-técnica;
- **Ferramentas**: Aumentar a adoção de soluções de automação para processos críticos, como gerenciamento de consentimentos e avaliações de impacto, reduzindo a carga operacional.

5.2. Limitações e Trabalhos Futuros

As limitações deste trabalho, como a substituição de entrevistas por questionários, já foram discutidas na seção de *Ameaças à Validade*, mas lacunas práticas em escala (ex.: subutilização de PIAs) foram possíveis de serem identificadas como discutidas anteriormente. Futuros estudos poderiam combinar métodos qualitativos para explorar motivações por trás da baixa adoção de *frameworks*, além de análises longitudinais para monitorar a evolução da LGPD em diferentes setores. Então, sugere-se:

- Combinar entrevistas qualitativas com desenvolvedores e gestores para explorar motivações por trás da baixa adoção de padrões como a ISO 27701;
- Realizar estudos de caso em organizações que adotaram estratégias bem-sucedidas, mapeando processos replicáveis;
- Realização de pesquisas considerando recortes regionais, por motivo de profissionais de uma cidade poder ter um conhecimento superior do que profissionais de outra, por exemplo;
- Integrar privacidade em currículos de TI e promover certificações técnicas para desenvolvedores, como proposto por [Canedo et al. 2022];
- Acompanhar a evolução da adoção da LGPD em diferentes setores, analisando o impacto de iniciativas educacionais e regulatórias.

5.3. Considerações Finais

Este estudo buscou explorar as percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software no contexto brasileiro, sob a vigência da LGPD. Embora os resultados revelem *insights* relevantes, é importante reconhecer que as conclusões derivam de uma amostra limitada (31 participantes) e de um recorte conceitual específico (questionários adaptados de um estudo internacional). Portanto, as generalizações devem ser feitas com cautela, e os achados representam um passo inicial para compreender um tema complexo e em constante evolução. As contribuições deste trabalho residem na identificação de lacunas práticas, como a desconexão entre o conhecimento teórico sobre a LGPD e a adoção de metodologias sistêmicas (ex.: *Privacy by Design*), além da

ênfase em desafios organizacionais comuns, como a falta de clareza legal e a resistência à mudança. No entanto, longe de esgotar o debate, esses resultados destacam a necessidade de investigações mais aprofundadas, especialmente com amostras diversificadas e abordagens metodológicas mistas (quantitativas e qualitativas). É reconhecido que as limitações do estudo, como a ausência de entrevistas em profundidade, podem ter restringido a compreensão de nuances contextuais. Ainda assim, espera-se que este trabalho inspire iniciativas práticas, como a integração de treinamentos técnicos em privacidade em ambientes acadêmicos e corporativos, e estimule diálogos entre desenvolvedores, gestores e reguladores. A LGPD, como marco regulatório, exige esforços coletivos e contínuos para que seus princípios se traduzam em proteção efetiva de dados. Por fim, este estudo pretende contribuir para um diálogo mais estruturado sobre privacidade no desenvolvimento de software no Brasil. Pesquisas futuras, aliadas a políticas públicas e investimentos em educação técnica, serão essenciais para transformar desafios identificados em oportunidades de avanço.

Referências

Bambauer, D. E. (2013). Privacy versus security. *J. Crim. L. & Criminology*, 103:667.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acessado: 2025-03-20.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101.

Canedo, E. D., Calazans, A. T. S., Bandeira, I. N., Costa, P. H. T., and Masson, E. T. S. (2022). Guidelines adopted by agile teams in privacy requirements elicitation after the brazilian general data protection law (lgpd) implementation. *Requirements Engineering*, 27(4):545–567.

Carver, J. C. (2010). Towards reporting guidelines for experimental replications: A proposal. In *1st international workshop on replication in empirical software engineering*, volume 1, pages 1–4.

Carver, J. C., Juristo, N., Baldassarre, M. T., and Vegas, S. (2014). Replications of software engineering experiments.

de Jesus, E. D. B., Vilela, J., and Silva, C. (2024). Requisitos de segurança e privacidade em startups: Um estudo empírico em uma aplicação de governança de dados.

de Melo, R. O. P., Vilela, J., and Silva, C. (2024). Do entendimento à aplicação: Requisitos de privacidade e a visão dos usuários sobre a lgpd.

Dennis, A. R. and Valacich, J. S. (2015). A replication manifesto. *AIS Transactions on Replication Research*, 1(1):1.

ENTERPRISE, I. P. T. (2020). Nist privacy framework: A tool for improving privacy through enterprise risk management, version 1.0.

European Parliament and Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL. Acessado: 2025-03-20.

Experian, S. (2020). Pesquisa lgpd (lei geral de proteção a dados). https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf. Acessado: 2025-03-20.

ISO/IEC (2019). Iso/iec 27701:2019. Standard, International Organization for Standardization.

Iwaya, L. H., Babar, M. A., and Rashid, A. (2023). Privacy engineering in the wild: Understanding the practitioners' mindset, organizational aspects, and current practices. *IEEE Transactions on Software Engineering*, 49(9):4324–4348.

Kilhoffer, Z., Wilder, D., and Bashir, M. (2024). Compliance as baseline, or striving for more? how privacy engineers work and use privacy standards. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 9–18. IEEE.

Peixoto, M., Ferreira, D., Cavalcanti, M., Silva, C., Vilela, J., Araújo, J., and Gorschek, T. (2023). The perspective of brazilian software developers on data privacy. *Journal of Systems and Software*, 195:111523.

Spiekermann, S., Korunovska, J., and Langheinrich, M. (2018). Inside the organization: Why privacy and security engineering is a challenge for engineers. *Proceedings of the IEEE*, 107(3):600–615.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., Wesslén, A., et al. (2012). *Experimentation in software engineering*, volume 236. Springer.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired*, pages 203–213. Routledge.

6. Apêndice

Questionário: Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software

Prezado participante,

Por meio deste questionário, convidamos você a participar da pesquisa "Percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software".

Esta pesquisa pertence a um trabalho de conclusão de curso de graduação do Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE).

Na próxima seção, você encontrará informações detalhadas sobre os objetivos, procedimentos, e seus direitos como participante.

Caso você decida participar, o tempo estimado para responder este questionário é, aproximadamente, **10 minutos**.

Contato: Se você tiver dúvidas ou quiser mais informações sobre a pesquisa, pode entrar em contato com Manoel Alves (Estudante de Graduação do curso de Engenharia da Computação - CIn/UFPE) pelo e-mail maxn@cin.ufpe.br.

* Indica uma pergunta obrigatória

P1. What is your nationality? (Qual a sua nacionalidade?)*

P2. Please select the language you prefer to use to answer this survey. (Por favor, selecione o idioma que você prefere usar para responder esse questionário).*

Marcar apenas uma.

( ) English

( ) Português (Brasil)

Termo de Consentimento Livre e Esclarecido (TCLE) em concordância com a pesquisa

Prezado participante,

Qual o objetivo da Pesquisa?

O objetivo desta pesquisa é analisar as percepções, práticas e desafios relacionados à privacidade no desenvolvimento de software, incluindo a integração de privacidade no ciclo de desenvolvimento, o uso de metodologias e *frameworks*, as responsabilidades dos profissionais, os desafios enfrentados e as oportunidades de melhoria nas práticas de privacidade. A pesquisa visa fornecer *insights* para aprimorar a proteção de dados pessoais no contexto do desenvolvimento de software. Gostaríamos de convidá-lo a preencher esta pesquisa e/ou compartilhá-la em suas redes.

Quem pode participar da pesquisa?

Podem participar da pesquisa profissionais e estudantes da área de desenvolvimento de software que tenham algum envolvimento ou interesse em práticas de privacidade. Isso inclui:

- Desenvolvedores, engenheiros e arquitetos de software.
- Analistas de sistemas e gerentes de projetos de TI.
- Profissionais com experiência em privacidade, segurança de dados ou uso de IA/ML.
- Estudantes de graduação ou pós-graduação em áreas como Ciência da Computação, Engenharia de Software e Sistemas de Informação.

A diversidade de cargos e níveis de experiência contribui para uma visão ampla sobre as práticas de privacidade no setor.

O que você será solicitado a fazer?

Se você decidir participar desta pesquisa, será solicitado a preencher um questionário on-line, com duração estimada de 10 minutos, sobre suas percepções e práticas relacionadas à **privacidade no desenvolvimento de software**.

O questionário inclui 4 seções:

1. Perfil do Desenvolvedor – Perguntas sobre sua formação acadêmica, cargo atual e experiência profissional.
2. Práticas e Percepções sobre Privacidade – Perguntas sobre a integração de privacidade no ciclo de desenvolvimento e o uso de *frameworks* e ferramentas.
3. Responsabilidades e Desafios – Perguntas sobre desafios enfrentados e estratégias adotadas em projetos.

4. Melhorias e Recomendações – Perguntas sobre sugestões para aprimorar as práticas de privacidade.

O tempo total de resposta pode variar em torno de **10 minutos**.

Confidencialidade

Todas as informações fornecidas serão mantidas em sigilo e utilizadas exclusivamente para fins acadêmicos e científicos. Os resultados poderão ser publicados em trabalhos, artigos científicos ou apresentados em conferências, mas sempre de forma anônima e agregada, garantindo que nenhum participante seja identificado.

Gostaríamos de enfatizar que:

1. Sua participação é totalmente **voluntária** e **anônima**.
2. Nenhuma informação pessoal que permita a identificação será divulgada.
3. Você pode se retirar da pesquisa a qualquer momento, sem qualquer prejuízo ou penalização.

Ao prosseguir, você confirma que leu e compreendeu os termos acima e concorda em participar desta pesquisa.

Agradecemos sua colaboração!

Contato:

Se você tiver dúvidas ou quiser mais informações sobre a pesquisa, pode entrar em contato com Manoel Alves (Estudante de Graduação do curso de Engenharia da Computação - CIn/UFPE) pelo e-mail mailto:maxn@cin.ufpe.brmaxn@cin.ufpe.br.

P3. Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa. *

Marcar apenas uma.

( ) Aceito participar (Pular para a pergunta 5)

( ) Não aceito participar

Perfil do Desenvolvedor

O objetivo dessa seção é coletar informações sobre sua formação acadêmica, cargo atual e experiência profissional

P5. Qual é o seu nível de formação acadêmica? *

Marcar apenas uma.

( ) Estudante de graduação

( ) Graduação completa

( ) Pós-graduação lato sensu (Especialização)

( ) Estudante de mestrado

( ) Mestrado completo

( ) Estudante de doutorado

( ) Doutorado completo

P6. Qual é o seu curso ou área de formação? *

Marcar apenas uma.

( ) Ciência da Computação

( ) Engenharia de Software

( ) Engenharia da Computação

( ) Sistemas de Informação

( ) Direito

( ) Gestão ou Administração

( ) Engenharia (outras áreas)

( ) Ciências Sociais ou Humanas

( ) Outro:

P7. Qual é o seu cargo atual? *

Marcar apenas uma.

( ) Programador/Desenvolvedor de Software

( ) Engenheiro de Software

( ) Arquiteto de Software

( ) Analista de Sistemas

( ) Gerente de Projetos de TI

( ) Outro:

P8. Quantos anos de experiência você tem na área? *

Marcar apenas uma.

( ) Menos de 1 ano

( ) 1-3 anos

( ) 4-6 anos

( ) 7-10 anos

( ) 11-15 anos

( ) Mais de 15 anos

P9. Como você define **privacidade** e **segurança** no contexto de engenharia de software? *

Marcar apenas uma.

( ) Não tenho certeza do que é segurança.

( ) Não tenho certeza do que é privacidade.

( ) São conceitos semelhantes, com diferenças mínimas.

( ) Privacidade e segurança são conceitos distintos, mas inter-relacionados.

P10. Como você adquiriu seu conhecimento sobre privacidade de dados? (Selecione todas as opções que se aplicam): *

Marque todas que se aplicam.

[ ] Não possuo conhecimento sobre privacidade.

[ ] Durante o ciclo acadêmico (graduação, pós-graduação, etc.).

[ ] Treinamento interno fornecido pela empresa.

[ ] Cursos externos ou certificações (e.g., ISO 27701, LGPD).

[ ] Autoaprendizado (e.g., leitura de artigos, vídeos, pesquisas).

[ ] Experiência prática em projetos ou no trabalho.

[ ] Outro:

P11. Qual é o seu nível de conhecimento sobre a LGPD (Lei Geral de Proteção de Dados Pessoais)? *

Marcar apenas uma.

( ) Nenhum conhecimento.

( ) Conhecimento básico (noções gerais sobre a lei).

( ) Conhecimento intermediário (entendo os principais requisitos e impactos).

( ) Conhecimento avançado (aplico a LGPD em projetos ou no trabalho).

P12. Qual é o porte da sua organização? *

Marcar apenas uma.

( ) Pequena (menos de 100 funcionários)

( ) Média (100 a 500 funcionários)

( ) Grande (mais de 500 funcionários)

P13. Que tipo de sistema você desenvolve atualmente? *

Marcar apenas uma.

( ) Sistemas financeiros

( ) Sistemas de varejo ou e-commerce

( ) Plataformas educacionais

( ) Aplicações de big data e análise de dados

( ) Aplicações de saúde ou sistemas médicos

( ) Aplicações de inteligência artificial ou aprendizado de máquina

( ) Sistemas industriais ou IoT (Internet das Coisas)

( ) Jogos ou entretenimento digital

( ) Sistemas governamentais ou de serviços públicos

( ) Outro:

P14. Você trabalha de forma próxima com sua equipe/organização ou com os clientes? *

Marcar apenas uma.

( ) Sim, trabalho em estreita colaboração com minha equipe/organização para definir requisitos e implementar soluções.

( ) Sim, trabalho diretamente com os clientes para entender suas necessidades e adaptar soluções.

( ) Não, meu trabalho é mais independente, com pouca interação com a equipe/organização ou clientes.

( ) Não, mas minha equipe/organização trabalha diretamente com os clientes e eu apoio de forma indireta.

P15. Você utiliza ferramentas de IA/ML (como Modelos de Linguagem de Grande Escala) no seu trabalho? *

Marcar apenas uma.

( ) Sim, para análise de dados e geração de insights.

( ) Sim, para automação de tarefas repetitivas.

( ) Sim, para gerar código ou auxiliar no desenvolvimento de software.

( ) Sim, para criação de chatbots ou assistentes virtuais.

( ) Sim, para análise de sentimentos e processamento de linguagem natural.

( ) Não, não utilizo ferramentas de IA/ML no meu trabalho.

( ) Não, mas minha equipe/organização utiliza ferramentas de IA/ML.

P16. Quando você ou sua equipe/organização utilizam ferramentas de IA/ML (como Modelos de Linguagem de Grande Escala), vocês adotam práticas específicas para garantir a privacidade dos dados utilizados? *

Marcar apenas uma.

( ) Sim, sempre implementamos medidas para proteger dados pessoais e sensíveis, como anonimização e controle de acesso.

( ) Sim, tomamos medidas de segurança, mas enfrentamos desafios relacionados a dados sensíveis.

( ) Não, não temos uma abordagem formalizada para garantir a privacidade dos dados no uso de IA/ML.

( ) Não utilizamos dados pessoais ou sensíveis nos projetos com IA/ML.

( ) Não, não utilizo ferramentas de IA/ML no meu trabalho.

Práticas de Desenvolvimento e Percepções sobre Privacidade

O objetivo dessa seção é coletar informações sobre a integração de privacidade no ciclo de desenvolvimento e o uso de *frameworks* e ferramenta.

P17. Como a privacidade é integrada ao ciclo de desenvolvimento em sua organização? *

Marcar apenas uma.

( ) Desde o início, considerando a privacidade em todas as fases do desenvolvimento.

( ) Apenas em etapas específicas, como no planejamento ou na implementação.

( ) Não é uma prioridade no ciclo de desenvolvimento.

P18. Você utiliza metodologias ou *frameworks* para implementar privacidade, como *Privacy by Design* ou *Privacy Impact Assessments* (PIAs)? (Escolha todas as opções que se aplicam): *

Marque todas que se aplicam.

[ ] Sim, utilizamos *Privacy by Design* em todas as fases do desenvolvimento.

[ ] Sim, utilizamos *Privacy Impact Assessments* (PIAs) para avaliar o impacto de privacidade.

[ ] Não, não utilizamos essas metodologias.

[ ] Não sei o que são essas metodologias.

P19. Quais ferramentas ou estratégias sua equipe/organização utiliza para implementar a privacidade em seus projetos? (Escolha todas as opções que se aplicam): *

Marque todas que se aplicam.

[ ] Anonimização de dados

[ ] Minimização de dados

[ ] Controle de acesso

[ ] Consentimento informado

[ ] Nenhuma das opções acima

[ ] Outro:

P20. Quais padrões ou *frameworks* sua equipe/organização segue para garantir a conformidade com a privacidade? (Escolha todas as opções que se aplicam): *

Marque todas que se aplicam.

[ ] NIST *Privacy Framework*

[ ] ISO 27001 (série ISO 27000)

[ ] ISO 27701

[ ] LGPD (Lei Geral de Proteção de Dados Pessoais)

[ ] Padrões de Segurança e Privacidade da ANPD (Autoridade Nacional de Proteção de Dados)

[ ] GDPR (*General Data Protection Regulation*)

[ ] FedRAMP (*Federal Risk and Authorization Management Program*)

[ ] ISO/IEC 29100

[ ] CCPA (*California Consumer Privacy Act*)

[ ] PIPEDA (*Personal Information Protection and Electronic Documents Act*)

[ ] HIPAA (*Health Insurance Portability and Accountability Act*)

[ ] SOC 2 (*System and Organization Controls 2*)

[ ] Outro:

P21. As decisões relacionadas à privacidade no seu projeto geralmente: (Escolha todas as opções que se aplicam) *

Marque todas que se aplicam.

[ ] São definidas pela equipe de desenvolvimento

[ ] São influenciadas pelo cliente

[ ] Seguem apenas diretrizes legais

[ ] São baseadas em *frameworks* ou padrões como o NIST *Privacy Framework* ou ISO 27701

[ ] São definidas por um comitê ou equipe de privacidade específica

[ ] Outro:

P22. Com que frequência você recorre a padrões ou *frameworks* de privacidade em seu trabalho? *

Marcar apenas uma.

( ) Sempre

( ) Frequentemente

( ) Raramente

( ) Nunca

P23. Quais desafios você enfrenta ao integrar privacidade ao desenvolvimento de

software? (Escolha todas as opções que se aplicam) *

Marque todas que se aplicam.

[ ] Falta de recursos e tempo

[ ] Falta de clareza nos requisitos legais

[ ] Dificuldade em automatizar processos relacionados à privacidade

[ ] Resistência organizacional

[ ] Outro:

P24. Como você define ”privacidade”no contexto do desenvolvimento de software e como percebe a diferença em relação às expectativas dos usuários? (Escolha todas as opções que se aplicam) *

Marque todas que se aplicam.

[ ] Controle do usuário sobre seus dados

[ ] Proteção contra acessos não autorizados

[ ] Parte da segurança

[ ] Existe uma lacuna entre as expectativas dos usuários sobre privacidade e as práticas de desenvolvimento

[ ] Outro:

Responsabilidades e Desafio

O objetivo dessa seção é coletar informações sobre desafios enfrentados e estratégias adotadas em projetos.

P25. Você já enfrentou desafios ao implementar requisitos de privacidade? Se sim, qual(is)? *

Marque todas que se aplicam.

[ ] Falta de clareza nas diretrizes legais

[ ] Dificuldade em implementar práticas de privacidade desde o início do desenvolvimento

[ ] Conflitos entre as demandas de segurança e privacidade

[ ] Falta de treinamento ou conhecimento sobre privacidade

[ ] Não enfrentei desafios

[ ] Outro:

P26. Como você avalia o suporte organizacional para lidar com questões de privacidade? *

Marcar apenas uma.

( ) Suficiente

( ) Parcial

( ) Insuficiente

P27. Em sua organização, quem é responsável por definir estratégias de privacidade no desenvolvimento? *

Marque todas que se aplicam.

[ ] Desenvolvedores

[ ] Arquitetos

[ ] Equipes de compliance

[ ] Gestores ou líderes de TI

[ ] Cliente

[ ] Outro:

P28. Quando surgem conflitos entre requisitos de privacidade e demandas do cliente, o que geralmente acontece? *

Marcar apenas uma.

( ) A privacidade é priorizada

( ) As demandas do cliente prevalecem

( ) Uma solução intermediária é encontrada

( ) Outro:

P29. Sua equipe/organização utiliza automatização para lidar com solicitações de acesso ou exclusão de dados pessoais? *

Marcar apenas uma.

( ) Sim, totalmente automatizado

( ) Sim, parcialmente automatizado

( ) Não, é um processo manual

Melhorias e Recomendações

O objetivo dessa seção é coletar informações e sugestões para aprimorar as práticas de privacidade.

P30. O que sua organização poderia fazer para melhorar as práticas de privacidade? (Escolha todas as opções que se aplicam): *

Marque todas que se aplicam.

[ ] Treinamento e capacitação sobre privacidade e segurança de dados

[ ] Melhorar ferramentas e processos relacionados à privacidade

[ ] Prover maior clareza sobre responsabilidades em relação à privacidade

[ ] Desenvolver uma cultura de privacidade dentro da organização

[ ] Outro:

P31. Qual seria o principal benefício de incluir privacidade como um tópico central nos currículos acadêmicos de tecnologia? *

Marque todas que se aplicam.

[ ] Melhorar a conformidade legal com regulamentações como LGPD e GDPR

[ ] Facilitar a integração de práticas de privacidade nos projetos de tecnologia

[ ] Aumentar a conscientização sobre a importância da privacidade entre futuros desenvolvedores

[ ] Não acredito que incluir conteúdos sobre privacidade nos currículos de cursos de tecnologia seria benéfico

[ ] Outro:

P32. Sua organização fornece suporte suficiente para atualizar ferramentas e práticas relacionadas à privacidade? *

Marcar apenas uma oval.

( ) Sim, com recursos adequados e atualizações frequentes

( ) Parcialmente, com suporte limitado

( ) Não, há falta de recursos ou suporte adequado

P33. Há mais algo que você gostaria de compartilhar sobre privacidade no desenvolvimento de software?