
**UNIVERSIDADE FEDERAL DO CEARÁ**

**CAMPUS DE ITAPAJÉ**

**CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO**

**ARYELY MARIA SILVA MATOS**

# PRIVACIDADE DE DADOS NA PRÁTICA DE SOFTWARE: PERSPECTIVAS DE DESENVOLVEDORES BRASILEIROS

**ITAPAJÉ**

**2025**

ARYELY MARIA SILVA MATOS

# PRIVACIDADE DE DADOS NA PRÁTICA DE SOFTWARE: PERSPECTIVAS DE DESENVOLVEDORES BRASILEIROS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do Campus de Itapajé da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Segurança da Informação.

Orientador: Prof. Dr. Anderson Gonçalves Uchôa

Coorientadora: Profa. Dra. Juliana Alves Pereira

ITAPAJÉ

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

M381p Matos, Aryely Maria Silva.
Privacidade de Dados na Prática de Software: Perspectivas de Desenvolvedores Brasileiros / Aryely Maria Silva Matos. – 2025.
120 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Itapajé, Curso de Segurança da Informação, Fortaleza, 2025.
Orientação: Prof. Dr. Anderson Gonçalves Uchôa.
Coorientação: Profa. Dra. Juliana Alves Pereira.

1. Privacidade de Dados. 2. Desenvolvimento de Software. 3. Estratégias de Privacidade de Dados. 4. Fatores Organizacionais. 5. Conscientização. I. Título.

CDD 005.8

---

ARYELY MARIA SILVA MATOS

PRIVACIDADE DE DADOS NA PRÁTICA DE SOFTWARE: PERSPECTIVAS DE DESENVOLVEDORES BRASILEIROS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do Campus de Itapajé da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Segurança da Informação.

Aprovada em: 24 de Novembro de 2025

BANCA EXAMINADORA

---

Prof. Dr. Anderson Gonçalves Uchôa (Orientador)
Universidade Federal do Ceará (UFC)

---

Profa. Dra. Juliana Alves Pereira (Coorientadora)
Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)

Prof. Dr. João Henrique Gonçalves Medeiros Corrêa
Universidade Federal do Ceará (UFC)

Prof. Dr. Solon Alves Peixoto
Universidade Federal do Ceará (UFC)

A Deus, por ser meu alicerce.

À minha família, por serem a ponte que me permite realizar meus sonhos.

Aos amigos que trilharam comigo esta jornada.

## AGRADECIMENTOS

A minha família, em especial a minha avó, Lúcia Mesquita, a quem carinhosamente chamo de mãe, obrigada por me dar a oportunidade, a liberdade e a estrutura necessárias para que eu pudesse escolher e trilhar meus próprios caminhos.

Ao meu orientador, Professor Anderson Uchôa, por me escolher, acreditar em mim e exercer, com tanto zelo, paciência e excelência, o seu papel de orientador; e por cobrar de mim excelência, mesmo quando eu acreditava não ter capacidade. Sem sua orientação próxima, este trabalho não teria a mesma qualidade. À minha coorientadora, Profa. Juliana Alves Pereira, que, mesmo morando em outro estado, não deixou que a distância dificultasse a comunicação. Seu cuidado, observação e empenho permitiram que este trabalho fosse lapidado da melhor forma possível. Foi uma honra poder trabalhar com você.

À Professora Edna Canedo e aos estudantes Mário Patrício e Maria Isabel Nicolau, por contribuírem com tanto zelo para este trabalho. A ajuda de vocês foi fundamental para o bom desenvolvimento deste projeto. Foi muito bom aprender e colaborar com vocês. Aos participantes da banca examinadora, Professor João Henrique e Professor Solon Alves, obrigada por aceitarem meu convite. Sou grata por minha banca avaliadora ser composta por dois professores que admiro grandemente e que fizeram parte da minha formação.

Aos meus colegas, que hoje são grandes amigos – Adriel Bastos, Moniky Mendonça e Ruan de Lima – cada um de vocês tem um significado muito especial em minha vida acadêmica e pessoal. Minha experiência durante a graduação não teria sido tão positiva sem vocês. Aos meus amigos e amigas, Aline Kelly, Alexandre Lima, Helen Brandão, Luís Carlos, Elysson Alves, Rafaela Gomes e Josiele Matos, obrigada por me motivarem e incentivarem direta e indiretamente na execução deste trabalho. O cuidado e apoio de vocês tornam minha jornada mais leve e significativa.

Ao Programa de Educação Tutorial (PET), pela contribuição essencial durante meu período como bolsista, garantindo a estrutura necessária para que minha jornada na Universidade Federal do Ceará (UFC), Campus de Itapajé, fosse completa. A experiência no PET foi determinante para o desenvolvimento de habilidades fundamentais, que levarei não apenas para a academia, mas também para a vida.

Ao Laboratório de P&D em Ciência do Software e Integração de Dados (ResetLab.), ambiente que foi decisivo na minha jornada com a pesquisa científica, obrigada por proporcionar experiências, aprendizados e suporte fundamentais para meu desenvolvimento acadêmico. À UFC – Campus de Itapajé, por possibilitar o acesso ao ensino superior com excelência e oferecer professores capacitados, contribuindo de forma decisiva para minha formação acadêmica e pessoal.

“Depois do medo, vem o mundo.”

(Clarice Lispector)

## RESUMO

A privacidade de dados é um princípio essencial da segurança da informação, que visa proteger dados confidenciais contra acesso não autorizado e vazamento de informações. À medida que os sistemas de *software* avançam, o volume de informações pessoais também cresce exponencialmente. Portanto, incorporar práticas de engenharia de privacidade durante o desenvolvimento é vital para garantir a integridade dos dados, a confidencialidade e a conformidade com as regulamentações legais, como a Lei Geral de Proteção de Dados. No entanto, há uma lacuna no entendimento da conscientização dos desenvolvedores sobre a privacidade de dados, suas percepções sobre a implementação de estratégias de privacidade e a influência de fatores organizacionais nessa adoção. Assim, este estudo tem como objetivo explorar o nível de conscientização entre os desenvolvedores brasileiros em relação à privacidade de dados e suas percepções sobre as estratégias de implementação adotadas para garantir a privacidade de dados. Além disso, busca-se entender como os fatores organizacionais influenciam a adoção de práticas de privacidade de dados. Para isso, foi aplicado um questionário com 88 desenvolvedores brasileiros com experiência profissional relacionada à privacidade. O questionário incluiu 21 afirmações agrupadas em três tópicos para medir a conscientização dos desenvolvedores brasileiros sobre a privacidade de dados em software. A análise estatística revela diferenças substanciais entre os grupos, por exemplo, desenvolvedores com experiência profissional direta *versus* indireta relacionada à privacidade de dados. Os resultados também indicaram algumas estratégias de privacidade de dados, por exemplo, a criptografia, que são amplamente utilizadas e consideradas altamente importantes, enquanto outras, como desativar a coleta de dados, destacam estratégias em que a facilidade de uso não leva necessariamente à adoção generalizada. Por fim, identificou-se que a ausência de equipes dedicadas à privacidade está correlacionada com uma menor percepção de prioridade e menos investimento em ferramentas. Mesmo em organizações que reconhecem a importância da privacidade. As evidências obtidas oferecem percepções sobre

como os desenvolvedores brasileiros percebem e implementam práticas de privacidade de dados, enfatizando o papel crítico que a cultura organizacional desempenha na tomada de decisões relacionadas à privacidade. Espera-se que nossas descobertas contribuam para melhorar as práticas de privacidade na comunidade de desenvolvimento de software, particularmente em contextos semelhantes ao do Brasil.
**Palavras-chave:** privacidade de dados; desenvolvimento de software; estratégias de privacidade de dados; fatores organizacionais; conscientização.

## ABSTRACT

Data privacy is an essential principle of information security, aimed at protecting sensitive data from unauthorized access and information leaks. As software systems advance, the volume of personal information also grows exponentially. Therefore, incorporating privacy engineering practices during development is vital to ensure data integrity, confidentiality, and compliance with legal regulations, such as the General Data Protection Law (LGPD). However, there is a gap in understanding developers' awareness of data privacy, their perceptions of implementing privacy strategies, and the influence of organizational factors on this adoption. Thus, this paper aims to explore the level of awareness among Brazilian developers regarding data privacy and their perceptions of the implementation strategies adopted to ensure data privacy. Additionally, we seek to understand how organizational factors influence the adoption of data privacy practices. To this end, we surveyed 88 Brazilian developers with privacy-related work experience. We got 21 statements grouped into three topics to measure the Brazilian developers' awareness of data privacy in software. Our statistical analysis reveals substantial gaps between groups, e.g., developers have Direct v.s. Indirect data privacy-related work experience. We also reveal some data privacy strategies, e.g., Encryption, are both widely used and perceived as highly important; others, such as turning off data collection, highlight strategies where ease of use does not necessarily lead to widespread adoption. Finally, we identified that the absence of dedicated privacy teams correlates with a lower perceived priority and less investment in tools. Even in organizations that recognize the importance of privacy. Our findings offer insights into how Brazilian developers perceive and implement data privacy practices, emphasizing the critical role organizational culture plays in decision-making regarding privacy. We hope that our findings will contribute to improving privacy practices within the software development community, particularly in contexts similar to Brazil.

**Keywords:** data privacy; software development; data privacy strategies; organizational factors; awareness.

## LISTA DE FIGURAS

## LISTA DE TABELAS

## LISTA DE QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| GDPR | *General Data Protection Regulation* |
| GQM | *Goal-Question-Metric* |
| GT | *Grounded Theory* |
| IA | Inteligência Artificial |
| KAB | *Knowledge-Attitude-Behaviour* |
| LGPD | Lei Geral de Proteção de Dados |
| PbD | *Privacy by Design* |
| TCLE | Termo de Consentimento Livre e Esclarecido |
| TIC | Tecnologia da Informação e Comunicação |

## LISTA DE SÍMBOLOS

| | |
|---|---|
| $i$ | Índice do participante da pesquisa. |
| $j$ | Índice da estratégia de privacidade de dados. |
| $W(i)$ | Peso total atribuído ao participante $i$. |
| $E(i)$ | Nível acadêmico mais alto do participante $i$. |
| $S(i)$ | Nível de senioridade do participante $i$ em sua posição atual. |
| $Y(i)$ | Número de anos de experiência em desenvolvimento de software do participante $i$. |
| Mediana$(Y)$ | Mediana dos anos de experiência em desenvolvimento de software considerando todos os participantes. |
| $R(i)$ | Valor da relação entre experiência direta e especialização em privacidade de dados do participante $i$. |
| $D(i)$ | Indicador de experiência direta em privacidade de dados (1 = possui; 0 = não possui). |
| $X(i)$ | Indicador de especialização profissional em privacidade de dados (1 = especialista; 0 = não especialista). |
| $T(j)$ | Valor total ponderado da frequência de uso, importância percebida ou facilidade de uso para a estratégia de privacidade de dados $j$. |
| Resposta$(i, j)$ | Valor da resposta do participante $i$ para a estratégia $j$, variando de 1 a 5. |
| $N(j)$ | Valor normalizado (0–100%) da frequência de uso, importância percebida ou facilidade de uso para a estratégia de privacidade de dados $j$. |
| $PontMaxPorParticipante$ | Pontuação máxima que um participante pode fornecer em uma escala Likert (por exemplo, 5). |

| | |
|---|---|
| $n$ | Número total de participantes da pesquisa. |

**SUMÁRIO**

# 1 INTRODUÇÃO

A crescente complexidade dos produtos e serviços de *software* introduziu desafios significativos para a engenharia de *software*, particularmente no que diz respeito à conformidade regulatória (KEMPE; MASSEY, 2021). As regulamentações voltadas para tecnologias como inteligência artificial ou que regem processos como o processamento de dados pessoais estão se tornando cada vez mais prevalentes e rigorosas, forçando as organizações a se adaptarem rapidamente. Além disso, os avanços no uso da Inteligência Artificial (IA) generativa despertaram uma demanda crescente por novas estruturas regulatórias especificamente adaptadas às aplicações de IA generativa. Como resultado, espera-se que a proliferação de leis e regulamentações se intensifique, abordando diversas preocupações que vão desde a privacidade dos dados dos usuários até questões éticas associadas ao uso de tecnologias emergentes (KSHETRI, 2024)

Para os desenvolvedores de *software*, esses cenários regulatórios em evolução exigem o alinhamento de suas práticas com princípios estruturados e a demonstração de conformidade para evitar penalidades, como multas substanciais ou até mesmo a retirada de produtos não conformes do mercado (PEIXOTO *et al.*, 2023). A privacidade de dados, em particular, surgiu como uma preocupação crítica para a conformidade regulatória, especialmente à luz das leis globais de proteção de dados, como a *General Data Protection Regulation* (GDPR) e a Lei Geral de Proteção de Dados (LGPD) do Brasil. Os engenheiros de *software* devem navegar por esses requisitos para garantir que os dados pessoais sejam tratados com responsabilidade ao longo do ciclo de vida de desenvolvimento de *software* (CANEDO *et al.*, 2023). No entanto, essa tarefa é frequentemente complicada por exigências regulatórias sobrepostas e interpretações variadas dos requisitos de privacidade e segurança. No centro da conformidade regulatória está a engenharia de requisitos de *software*, que traduz as exigências legais e regulatórias em requisitos acionáveis e testáveis. Apesar de sua importância, a literatura existente revela

uma falta de compreensão sistemática dos desafios e práticas relacionados à integração da privacidade de dados no desenvolvimento de *software*. Além disso, as regulamentações são projetadas para proteger os direitos dos indivíduos, regulando como os dados pessoais são coletados, processados e armazenados, impondo requisitos rigorosos às organizações para que mantenham os padrões de privacidade (CANEDO *et al.*, 2023; PEIXOTO *et al.*, 2023).

A importância de enfrentar os desafios associados à garantia da privacidade dos dados dos usuários vai muito além de evitar penalidades. A conformidade com as regulamentações de privacidade de dados serve como base para construir a confiança dos usuários finais e das partes interessadas, especialmente à medida que as preocupações com violações de dados e uso indevido de informações pessoais continuam a crescer. Os desenvolvedores devem navegar por múltiplas estruturas regulatórias, muitas vezes sobrepostas, originárias de diferentes jurisdições, cada uma com seu escopo e requisitos únicos (FERRÃO *et al.*, 2024). Essa complexidade destaca a necessidade crítica de abordagens estruturadas para gerenciar a conformidade e incorporar considerações de privacidade nas práticas de engenharia de *software*. Ao fazer isso, as organizações podem não apenas atender aos requisitos legais, mas também promover a confiança e demonstrar seu compromisso com o gerenciamento ético de dados em um mundo cada vez mais consciente da privacidade (SANGAROONSILP *et al.*, 2023).

Ao priorizar a privacidade e a conformidade regulatória, as organizações não apenas mitigam os riscos, mas também se posicionam competitivamente no mercado, demonstrando seu compromisso com práticas éticas e responsáveis de gerenciamento de dados. Para os desenvolvedores, dominar esses desafios é essencial para fornecer produtos e serviços de *software* que não apenas estejam em conformidade legal, mas também alinhados com as expectativas sociais e os padrões éticos. Isso torna a conformidade regulatória um pilar da engenharia de *software* sustentável e responsável na economia digital atual (LANDIS; KROLL, 2024).

Este estudo visa preencher essa lacuna por meio da realização de uma pesquisa com 88 desenvolvedores brasileiros com experiência profissional relacionada à privacidade. Com base no modelo *Knowledge-Attitude-Behaviour* (KAB) (SCHRADER; LAWLESS, 2004), foram explorados aspectos-chave da conscientização dos desenvolvedores, incluindo a compreensão dos princípios, leis e melhores práticas de privacidade de dados; as atitudes em relação à privacidade de dados; e os comportamentos e ações reais relacionados à privacidade. Além disso, foram analisadas as percepções sobre 13 estratégias de implementação e a influência de fatores organizacionais nas práticas de privacidade de dados. Ao se concentrar no contexto brasileiro, esta pesquisa fornece *insights* valiosos sobre os desafios que os desenvolvedores enfrentam para alinhar suas práticas com as regulamentações de privacidade de dados.

## 1.1 Objetivos

A privacidade de dados no processo de desenvolvimento de *software*, embora muito importante, ainda apresenta lacunas que merecem investigação, como o nível de conscientização dos desenvolvedores, a influência da cultura organizacional e o uso de estratégias de privacidade voltadas à proteção de dados em sistemas. Diante desse cenário, é de suma importância compreender esses fatores e suas relações, a fim de contribuir para a identificação de elementos que orientam a aplicação da privacidade de dados no desenvolvimento de sistemas. Assim, nas Subseções 1.1.1 e 1.1.2 serão apresentados, respectivamente, o objetivo geral e os objetivos específicos que nortearam este estudo.

### *1.1.1 Objetivo Geral*

Explorar como os desenvolvedores de *software* brasileiros compreendem e aplicam aspectos relacionados à privacidade de dados ao longo do processo de desenvol-

vimento, desde a fase de concepção, identificando as estratégias de privacidade utilizadas, bem como analisando a influência de fatores organizacionais nessa adoção.

### *1.1.2 Objetivos Específicos*

A fim de operacionalizar o objetivo geral e aprofundar a compreensão sobre diferentes aspectos da privacidade de dados, este estudo foi conduzido a partir dos seguintes objetivos específicos:

a) Compreender o grau de conscientização dos desenvolvedores sobre o conceito de *Privacy by Design*;
b) Identificar fatores relacionados ao uso, à facilidade e à frequência de adoção das estratégias de privacidade de dados pelos desenvolvedores.
c) Analisar como os fatores organizacionais influenciam a adoção de práticas de privacidade nas equipes de desenvolvimento; e
d) Investigar em quais fases do desenvolvimento os desenvolvedores aplicam estratégias de privacidade de dados.

### *1.1.3 Questões de Pesquisa*

Com o propósito de atingir os objetivos desta pesquisa, propomos as seguintes Questões de Pesquisa (QP):

a) **QP1:** Até que ponto os desenvolvedores estão cientes da privacidade dos dados no desenvolvimento de *software*?
b) **QP2:** Como as percepções dos desenvolvedores sobre frequência, importância e facilidade de uso diferem para várias estratégias de privacidade de dados?
c) **QP3:** Como os fatores organizacionais influenciam a adesão às práticas de privacidade de dados nas equipes de desenvolvimento?

## 1.2 Contribuições do Estudo

Os dados e resultados apresentados neste Trabalho de Conclusão de Curso são baseados na publicação aceita no *Journal of Internet Services and Applications* (JISA) (MATOS *et al.*, 2025), refletindo a consolidação e a validação científica dos achados obtidos. Além disso, todos os dados, incluindo *scripts*, *survey script*, as análises estatísticas e o *codebook* completo das perguntas abertas, estão disponíveis no repositório Zenodo (<https://doi.org/10.5281/zenodo.14345392>), um repositório online que permite o compartilhamento de publicações e dados de apoio para fins de replicação e reuso científico. Essa disponibilização garante transparência, reprodutibilidade e suporte a futuras pesquisas na área.

As contribuições desse estudo incluem: (i) *insights* sobre os termos mais frequentes que os desenvolvedores brasileiros associam à privacidade de dados; (ii) uma análise de evidências empíricas destacando pontos fortes e lacunas da conscientização de desenvolvedores sobre privacidade de dados; (iii) conclusões sobre as percepções dos desenvolvedores brasileiros em relação a várias estratégias de privacidade de dados, com foco na frequência de uso, importância percebida e facilidade de implementação; e (iv) uma discussão sobre como as estruturas organizacionais, prioridades e recursos afetam a adoção e a aplicação de práticas de privacidade de dados nas equipes de desenvolvimento.

De forma geral, os resultados obtidos evidenciam lacunas e padrões relevantes relacionados à aplicação da privacidade de dados no desenvolvimento de *software*. As análises revelam tanto aspectos conceituais quanto fatores organizacionais e práticos que influenciam a adoção de estratégias de privacidade. Os achados indicam que a privacidade de dados ainda é amplamente associada à segurança da informação e aplicada de forma reativa, concentrando-se principalmente nas fases de codificação e testes. Sua adoção varia conforme a experiência do desenvolvedor e o porte organizacional, apresentando correlação entre importância, frequência e facilidade de uso. Observa-se,

ainda, a necessidade de maior adesão a leis como a LGPD, de implementação de equipes de conformidade e de investimento em capacitação, além de desafios crescentes devido ao avanço de tecnologias como a inteligência artificial.

## 1.3 Organização do Trabalho

Este trabalho está estruturado da seguinte forma: No Capítulo 2 é abordado a fundamentação teórica, discutindo conceitos importantes relacionados à privacidade de dados e segurança de *software*. No Capítulo 3 é apresentado os principais trabalhos relacionados, fornecendo uma base comparativa e evidenciando possíveis lacunas na literatura. Já no Capítulo 4 são descritos os processos metodológicos utilizados no desenvolvimento deste estudo. No Capítulo 5 é apresentado e analisado os principais resultados obtidos. Já no Capítulo 6 é apresentado possíveis ameaças à validade. Por fim, o Capítulo 7 traz as conclusões gerais, as principais conclusões do trabalho e sugestões para estudos futuros.

## 1.4 Resumo do Capítulo 1

Neste capítulo é realizada uma introdução ao tema, com a devida contextualização do problema e a ênfase na relevância da pesquisa. São apresentados o objetivo geral e os objetivos específicos, bem como as questões de pesquisa que orientaram o desenvolvimento do estudo. Destacam-se, ainda, as principais contribuições pretendidas, tanto sob a perspectiva teórica quanto sob a perspectiva prática, especialmente no que se refere aos aspectos relacionados à privacidade de dados em *software*. Por fim, descreve-se a organização do trabalho de conclusão de curso, detalhando-se a estrutura dos capítulos e a lógica adotada para a condução do estudo. Na sequência, é apresentado o capítulo de fundamentação teórica, no qual são discutidos os principais trabalhos relacionados ao tema, que servem de base conceitual para a pesquisa desenvolvida.

# 2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta uma visão geral da base teórica para a compreensão dos principais conceitos do estudo, conforme a seguir. Esta seção está organizada em três partes principais. Na Seção 2.1 é apresentada uma discussão sobre a relação entre privacidade e segurança de *software*, destacando suas principais diferenças conceituais e complementares. Já na Seção 2.2 é abordado a importância da privacidade de dados em todo o processo de desenvolvimento de *software*, com foco em práticas e desafios vivenciados por desenvolvedores. Por fim, na Seção 2.3 é descrito as principais estratégias e abordagens de engenharia de privacidade, que servem como base conceitual para as análises e discussões apresentadas neste estudo.

## 2.1 Privacidade vs Segurança de Software

A distinção entre os termos privacidade e segurança de *software* é essencial, especialmente no contexto do desenvolvimento de *softwares* que lidam com dados pessoais. Embora frequentemente utilizados como sinônimos, esses conceitos possuem propósitos e objetivos diferentes dentro da engenharia de *software* e da segurança da informação. O termo privacidade é frequentemente confundido com segurança, o que é compreensível, uma vez que a privacidade constitui um componente essencial dentro do domínio da segurança da informação.

No estudo de Tahaei *et al.* (2021), especialistas em privacidade foram convidados a definir o conceito de privacidade de dados, e a maioria o descreveu como a proteção de informações pessoais contra acesso não autorizado. Por outro lado, conforme descrito por Lester e Jamerson (2009), a segurança de *software* é entendida como a capacidade de um sistema resistir, tolerar e se recuperar de eventos que ameaçam intencionalmente sua confiabilidade, preservando a disponibilidade, integridade e confidencialidade das informações.

Embora os conceitos de privacidade e segurança sejam distintos, eles estão intimamente relacionados: a segurança fornece os meios técnicos para viabilizar a proteção da privacidade, enquanto a privacidade estabelece os princípios éticos e legais que orientam o uso adequado das informações. Essa correlação, contudo, nem sempre é compreendida pelos desenvolvedores, que frequentemente tratam a privacidade como um simples requisito de segurança. Dessa forma, este estudo busca investigar como os desenvolvedores brasileiros percebem a privacidade de dados, explorando associações imediatas e conceitos-chave que orientam suas práticas.

## 2.2 Privacidade no Processo de Desenvolvimento de Software

A privacidade no processo de desenvolvimento de *software* é frequentemente associada à *Privacy by Design* (PbD) (HADAR *et al.*, 2018), uma estrutura que orienta os desenvolvedores, durante o processo de desenvolvimento, na aplicação de soluções e estratégias destinadas a garantir a proteção da privacidade. Em outras palavras, a PbD assegura que a privacidade dos dados seja integrada a todo o ciclo do desenvolvimento de *software*, desde a concepção inicial até a manutenção do sistema. Nesse contexto, a necessidade de garantir a proteção de dados tornou-se ainda mais evidente com a introdução de regulamentações como a GDPR na União Europeia (União Europeia, 2016) e, posteriormente, a LGPD no Brasil (BRASIL, 2018). Ambas as legislações estabelecem princípios e diretrizes sobre o tratamento e armazenamento de dados pessoais, além de incentivarem a aplicação de práticas de segurança e transparência ao longo do desenvolvimento de sistemas.

Dessa forma, a PbD deixa de representar apenas uma diretriz de boas práticas e passa a ser um princípio essencial para a conformidade legal e ética no ciclo de desenvolvimento de *software*. No entanto, apesar de sua necessidade e importância ser amplamente reconhecida na teoria e reforçada por legislações como a GDPR e a LGPD, ainda é necessário entender como esse princípio é de fato percebido e aplicado

por desenvolvedores de *software* na prática. Assim, este estudo explora a conscientização dos desenvolvedores brasileiros sobre a privacidade de dados, com foco em: (i) seu conhecimento dos princípios, leis e melhores práticas de privacidade; (ii) suas atitudes em relação à privacidade, incluindo crenças, valores e respostas emocionais; e (iii) suas ações em relação à privacidade de dados.

## 2.3 Práticas de Engenharia da Privacidade

A engenharia da privacidade é um campo multidisciplinar que surgiu como uma extensão prática integrando aspectos técnicos e organizacionais para incorporar a proteção de dados desde as fases iniciais do projeto até a manutenção de sistemas. Em outras palavras, a engenharia da privacidade inclui tanto recursos técnicos quanto processos de gestão voltados à privacidade. Entre esses princípios, destacam-se o uso de estratégias de implementação, que buscam garantir a proteção dos dados pessoais ao longo de todo o ciclo de desenvolvimento de *software*.

Um exemplo clássico é o uso da *Criptografia*, que protege os dados convertendo-os em um formato ilegível para partes não autorizadas, garantindo confidencialidade e a integridade das informações. Conforme discutido por Iwaya *et al.* (2023), diferentes estratégias de privacidade de dados podem ser adotadas dependendo do contexto e dos requisitos específicos do sistema que está sendo desenvolvido, pois cada estratégia oferece vantagens particulares diante de diferentes desafios de proteção de dados.

O Quadro 1 apresenta uma visão geral de treze estratégias de privacidade de dados comumente utilizadas por desenvolvedores, cada uma desempenhando um papel específico conforme as necessidades do sistema e as exigências regulatórias aplicáveis (STALLINGS, 2019). Neste estudo investigamos como os desenvolvedores brasileiros percebem a frequência, a importância e a facilidade de uso dessas estratégias, com o objetivo de compreender suas preferências, desafios e prioridades na aplicação da prática da engenharia da privacidade conforme a sua experiência. Essa análise busca oferecer

*insights* para aprimorar as práticas profissionais e orientar decisões no desenvolvimento de sistemas mais alinhados à proteção de dados e seus princípios.

Quadro 1 – Estratégias de privacidade de dados e suas descrições

| Estratégia | Descrição |
|---|---|
| **1. Criptografia** | Técnica usada para proteger informações, tornando-as inacessíveis a indivíduos não autorizados. Ela converte dados legíveis (texto simples) em um formato ilegível (texto cifrado). |
| **2. Minimização da coleta de dados pessoais** | Refere-se à prática de limitar a quantidade de dados pessoais coletados pela organização. |
| **3. Descentralização** | Envolve a distribuição da coleta, armazenamento e processamento de dados entre diferentes locais ou sistemas. |
| **4. Soberania dos dados** | Baseia-se no respeito às leis e regulamentos de proteção de dados em diferentes jurisdições. |
| **5. Dados temporais** | Refere-se ao uso e armazenamento de dados apenas pelo tempo necessário. |
| **6. Controle do usuário** | Envolve dar aos usuários controle sobre seus próprios dados, permitindo que eles acessem, modifiquem e excluam suas informações pessoais conforme necessário. |
| **7. Desativação da coleta de dados** | Consiste em fornecer opções para os usuários optarem por não participar da coleta de dados, respeitando suas preferências de privacidade. |
| **8. Anonimização** | Envolve remover ou alterar informações de identificação pessoal para que os dados não possam ser associados a indivíduos específicos. |
| **9. Ferramentas de classificação de dados** | São sistemas ou *softwares* usados para classificar e catalogar dados organizacionais, facilitando o gerenciamento e a identificação de informações confidenciais ou pessoais. |
| **10. Revisões de design e código** | Práticas que garantem que o processo de desenvolvimento esteja em conformidade com técnicas que garantem a segurança durante todo o processo de desenvolvimento. |
| **11. Gerenciamento de riscos** | Envolve avaliar e planejar os riscos associados ao processamento de dados. |
| **12. Modelagem de fluxo de dados** | Técnica usada para representar visualmente o movimento de dados dentro de um sistema de informação. |
| **13. Proxy** | Um proxy é usado para todas as solicitações a serviços de terceiros para ocultar a identidade dos usuários e impedir que terceiros obtenham informações sobre eles. |

Fonte: Elaborada pela autora (2025).

## 2.4 Resumo do Capítulo 2

Neste capítulo foram abordados os conceitos acerca de privacidade de dados, segurança no desenvolvimento de *software* e práticas de engenharia de privacidade, que integram a base conceitual desse estudo. Com base nisso, observa-se que a segurança de *software*, ainda que fundamental, não garante necessariamente privacidade dos dados, o que reforça a necessidade de abordagens de desenvolvimento que incorporem princípios de privacidade desde a concepção. Dessa forma, o presente estudo busca compreender como desenvolvedores de *software* percebem e aplicam estratégias de privacidade de dados em seus projetos de desenvolvimento, tomando como referência os princípios discutidos. A literatura aponta a importância dos princípios norteados pelo conceito do PbD, mas ainda há lacunas sobre sua adoção prática no contexto de desenvolvimento de *software*, lacuna que este estudo pretende explorar. Desse modo, com base nos conceitos aqui apresentados, o capítulo a seguir apresenta os trabalhos relacionados, destacando como diferentes estudos têm explorado a integração da privacidade de dados no processo de desenvolvimento e quais lacunas ainda permanecem na literatura.

# 3 TRABALHOS RELACIONADOS

A privacidade de dados, cuja importância vem crescendo no contexto do desenvolvimento de *software*, tem sido foco de estudos recentes que investigam os desafios relacionados a fatores organizacionais e às percepções de desenvolvedores na implementação de estratégias de privacidade de dados. Hadar *et al.* (2018), Tahaei *et al.* (2021), Iwaya *et al.* (2023) conduziram entrevistas com desenvolvedores para entender os desafios relacionados à garantia da privacidade de dados.

Esses estudos fornecem *insights* detalhados sobre estratégias de privacidade e os desafios enfrentados pelos desenvolvedores. No entanto, ainda existem lacunas na mensuração quantitativa desses fatores organizacionais e das percepções dos desenvolvedores. Para preencher essas lacunas, este estudo combina dados qualitativos e quantitativos coletados por meio de uma pesquisa estruturada, visando uma compreensão mais ampla dos fatores organizacionais que podem influenciar a adesão das equipes de desenvolvimento às práticas de privacidade. Dessa forma, nas próximas seções serão apresentados os estudos que contribuíram para o desenvolvimento deste trabalho. Para isso, foram selecionados os seguintes trabalhos Hadar *et al.* (2018); Canedo *et al.* (2023); Peixoto *et al.* (2023); Tahaei *et al.* (2021); Iwaya *et al.* (2023) que investigaram aspectos acerca da privacidade de dados em *software*.

## 3.1 *Privacy by Designers: Software Developers' Privacy Mindset*

Hadar *et al.* (2018) investigou as percepções e mentalidades de desenvolvedores de *software* em relação à privacidade desde o início do design (*Privacy by Design*). Os autores realizaram entrevistas com desenvolvedores para identificar e analisar suas percepções e práticas relacionadas à privacidade. Nosso estudo difere deste trabalho, pois conduzimos uma pesquisa com perguntas abertas e fechadas e realizamos análises quantitativas e qualitativas, permitindo alcançar um número maior de respondentes. Essa

abordagem contribui ativamente para compreender como as mentalidades e percepções dos desenvolvedores influenciam a adoção de estratégias de privacidade de dados nos sistemas que desenvolvem. O estudo de Hadar *et al.* (2018) é relevante para nosso trabalho, pois explora as percepções dos desenvolvedores sobre privacidade de dados, fornecendo um ponto de partida para analisar como fatores organizacionais e conhecimento técnico podem influenciar a aplicação de estratégias de privacidade em sistemas de *software*.

## 3.2 *Privacy Requirements Elicitation: A Systematic Literature Review and Perception Analysis of IT Practitioners*

Canedo *et al.* (2023) conduziu uma revisão sistemática da literatura para identificar metodologias, técnicas e ferramentas usadas para elicitação de requisitos de privacidade. Além disso, eles aplicaram uma pesquisa com profissionais de Tecnologia da Informação e Comunicação (TIC) para investigar suas percepções quanto ao uso dessas técnicas e ferramentas no processo de desenvolvimento de *software*. O estudo revelou que as metodologias, técnicas e ferramentas existentes para elicitação de requisitos de privacidade não são comumente utilizadas pelos profissionais da indústria. No entanto, os desenvolvedores reconheceram que seu uso poderia desempenhar um papel importante na garantia da privacidade de dados dos usuários. Este estudo difere do nosso, pois os autores focaram em investigar se as técnicas identificadas na literatura estavam sendo utilizadas na indústria, em vez de examinar como fatores organizacionais poderiam influenciar a adesão a essas técnicas e métodos.

## 3.3 *The Perspective of Brazilian Software Developers on Data Privacy*

Peixoto *et al.* (2023) investigou o nível de conhecimento e compreensão que os desenvolvedores de *software* possuem sobre privacidade, explorando fatores pessoais, comportamentais e do ambiente externo que influenciam suas decisões em relação aos

requisitos de privacidade. Eles realizaram entrevistas semiestruturadas com treze profissionais de seis empresas diferentes. O estudo identificou nove fatores pessoais, cinco fatores comportamentais e sete fatores do ambiente externo que impactam positivamente ou negativamente a tomada de decisão dos desenvolvedores sobre privacidade. Este trabalho difere do nosso, pois foca exclusivamente em fatores relacionados à fase de Engenharia de Requisitos, enquanto nosso estudo examina fatores ao longo de todo o ciclo de vida do desenvolvimento de *software*.

## 3.4 *Privacy Champions in Software Teams: Understanding their Motivations, Strategies, and Challenges*

Tahaei *et al.* (2021) analisou o papel dos *privacy champions* dentro das equipes de desenvolvimento de *software*. Esses profissionais são responsáveis por defender a privacidade dos dados dos usuários nas organizações, implementando estratégias de privacidade e lidando com desafios decorrentes da falta de privacidade de dados. Os autores conduziram entrevistas com esses profissionais para investigar suas motivações e as estratégias empregadas no contexto da privacidade de dados sensíveis nas organizações. Os resultados destacam que os *privacy champions* desempenham um papel importante ao aumentar a conscientização e promover a adoção de estratégias eficazes, apesar de enfrentarem barreiras como resistência cultural organizacional e restrições de recursos. Os autores enfatizam que contar com profissionais dedicados à privacidade pode fortalecer as melhores práticas no desenvolvimento de *software*, alinhando-as aos princípios de *Privacy by Design*. Este estudo está diretamente relacionado ao nosso, pois nosso objetivo é identificar os desafios e oportunidades na adoção de estratégias de privacidade entre desenvolvedores.

## 3.5 *Privacy Engineering in the Wild: Understanding the Practitioners' Mindset, Organizational Aspects, and Current Practices*

Alguns estudos também examinaram como aspectos organizacionais influenciam a adoção de estratégias de privacidade no desenvolvimento de *software*. Iwaya *et al.* (2023) investigou a percepção de desenvolvedores sobre privacidade, com foco em aspectos organizacionais. Os autores realizaram entrevistas com desenvolvedores e identificaram três dimensões-chave: conhecimento, atitudes e comportamentos dos desenvolvedores. Além disso, o estudo explorou como esses fatores influenciam a adoção de práticas de privacidade, bem como o impacto da liderança de equipe e da cultura organizacional na implementação dessas práticas. Um dos principais achados foi que culturas organizacionais negativas - caracterizadas pela baixa priorização da privacidade e pela ausência de incentivos para treinamentos - prejudicam diretamente a adoção de estratégias de privacidade. Apesar da crescente conscientização dos membros das equipes sobre privacidade de dados nos últimos anos, o tema ainda é pouco discutido, devido à falta de conhecimento sobre estratégias e padrões de engenharia de privacidade. Os autores também destacaram a importância da cultura organizacional e do papel da gestão na promoção do uso de estratégias de privacidade.

Os achados de Iwaya *et al.* (2023) se correlacionam com os de Hadar *et al.* (2018), que também enfatizam a importância de alinhar a cultura organizacional com as práticas adotadas pelos desenvolvedores para garantir a privacidade de dados. Ambos os estudos destacam a necessidade de iniciativas organizacionais mais robustas para fortalecer a cultura de privacidade, alinhando-se ao objetivo do nosso estudo de investigar como fatores organizacionais influenciam a adoção de estratégias de privacidade. Nosso estudo mede isso por meio da frequência, importância e uso das estratégias de privacidade pelas equipes de desenvolvimento de *software*.

## 3.6 Análise Comparativa

No Quadro 2 é apresentado um breve resumo comparativo dos trabalhos relacionados com o presente estudo. O quadro está dividido em: referência, objetivo, metodologia, número de participantes (N) e principais resultados.

Quadro 2 – Comparativo entre estudos relacionados sobre privacidade de dados em software

| **Referência** | **Objetivo** | **Metodologia** | **N** | **Principais resultados** |
|---|---|---|---|---|
| Hadar *et al.* (2018) | Investigar a percepção e mentalidade dos desenvolvedores de *software* com base no princípio do *Privacy by Design*. | Entrevistas semiestruturadas com desenvolvedores de *software*, atuando nas áreas de design e/ou arquitetura de *software*. | 27 | Desenvolvedores confundem privacidade com segurança; práticas moldadas pelo clima organizacional. |
| Canedo *et al.* (2021) (2021) | Investigar se técnicas de privacidade identificadas na literatura estavam sendo utilizados na industria. | Revisão sistemática da literatura + Aplicação de survey com profissionais de TI brasileiros. | 198 | Há desalinhamento entre o que a literatura propõe e o que é realmente usado na prática para elicitar (identificar) requisitos de privacidade em *software*. |
| Peixoto *et al.* (2023) | Investigar como desenvolvedores brasileiros percebem e aplicam práticas de privacidade de dados durante o desenvolvimento de *software*, além de identificar fatores que influenciam essa percepção. | Entrevistas semiestruturadas com profissionais de TI de empresas localizadas em Pernambuco. | 13 | Falta de tempo, cultura organizacional e desconhecimento da LGPD foram apontados como barreiras; o princípio do *Privacy by Design* é muito conhecido, mas pouco aplicado. |
| Tahaei *et al.* (2021) | Explorar quem são os "Privacy Champions" dentro das equipes de desenvolvimento de *software*, suas motivações, estratégias e desafios. | Entrevistas semiestruturadas com especialistas em privacidade. | 12 | Barreiras incluem cultura negativa, falta de métricas e ferramentas; destaca-se o valor do apoio gerencial. |
| Iwaya *et al.* (2023) | Explorar práticas, mentalidade e aspectos organizacionais da engenharia de privacidade. | Entrevistas semiestruturadas com 30 profissionais de segurança de 9 países | 30 | Cultura organizacional é determinante; práticas de privacidade ainda não são tratadas de forma sistemática. |
| Trabalho proposto | Investigar a percepção dos desenvolvedores e a influência de fatores organizacionais na adoção de estratégias de privacidade de dados. | *Survey* aplicado a desenvolvedores e analistas de segurança de *software*. | 88 | Estratégias como Criptografia, Descentralização e Controle do usuário são amplamente adotadas; A adoção de práticas varia conforme experiência, tamanho da organização e especialização profissional. |

Fonte: Elaborado pela autora (2025).

## 3.7 Resumo do Capítulo 3

Os estudos analisados evidenciam um crescente interesse na integração de práticas de privacidade ao processo de desenvolvimento de *software*, sobretudo por meio de diretrizes baseadas nos princípios de PbD. Apesar dos avanços observados, nota-se que a maioria dos estudos concentra-se em aspectos técnicos ou conceituais, havendo pouca ênfase na percepção dos desenvolvedores em relação a estratégias de privacidade no contexto real de desenvolvimento. Dessa forma, o presente estudo busca preencher essa lacuna ao investigar a percepção e o uso de estratégias de privacidade de dados por desenvolvedores de *software*, contribuindo para uma compreensão prática e contextualizada do tema. Com base nessa análise, no capítulo seguinte é apresentado a metodologia adotada para a condução da pesquisa, detalhando os procedimentos utilizados para a coleta e análise dos dados utilizados neste estudo.

# 4 METODOLOGIA

Este capítulo descreve a metodologia adotada neste estudo e está organizado da seguinte forma: Na Seção 4.1 é apresentado o objetivo do estudo e as questões de pesquisa. Em seguida, na Seção 4.2 é abordado o método de pesquisa utilizado e as etapas utilizadas, incluindo os procedimentos realizados para seleção dos participantes válidos e para a condução das análises qualitativas e quantitativas dos dados. Por fim, a Seção 4.3 traz as considerações finais do capítulo.

A metodologia proposta consiste em um estudo do tipo questionário, direcionado para a compreensão da percepção de desenvolvedores de *software* e especialistas em segurança da informação acerca da privacidade de dados no desenvolvimento de sistemas. O instrumento de coleta dos dados utilizado foi um questionário estruturado, elaborado com base na literatura já existente sobre o tema. Os dados coletados foram analisados de forma quantitativa e qualitativa: a análise quantitativa concentrou-se em técnicas estatísticas, enquanto a análise qualitativa empregou procedimentos de codificação aberta e axial, a fim de responder às questões de pesquisa propostas neste estudo.

## 4.1 Objetivo do Estudo e Questões de Pesquisa

Para definir o objetivo e as Questões de Pesquisa (**QPs**), foi utilizado o modelo *Goal-Question-Metric* (GQM) (CALDIERA; ROMBACH, 1994). Portanto, este estudo visa: **analisar** as estratégias de conscientização e implementação relacionadas à privacidade de dados entre desenvolvedores de *software*; **com o objetivo de** compreender sua conscientização e práticas relacionadas à privacidade de dados no desenvolvimento de software; **com relação a** aspectos-chave, como conscientização, percepção sobre estratégias de privacidade de dados e a influência de fatores organizacionais; **do ponto de vista de** pesquisadores; **no contexto de** desenvolvedores de software brasileiros. Detalhamos cada QP a seguir:

a) **$QP_1$: *Até que ponto os desenvolvedores estão cientes da privacidade dos dados no desenvolvimento de software?*** – $QP_1$ visa explorar a natureza multifacetada da consciência dos desenvolvedores sobre a privacidade dos dados. Para capturar essa consciência, 21 afirmações foram cuidadosamente elaboradas, e divididas em três tópicos principais: (i) *Conhecimento*, que avalia a compreensão e o conhecimento dos desenvolvedores sobre os princípios, leis e melhores práticas de privacidade de dados; (ii) *Atitudes e sentimentos*, que investiga as atitudes dos desenvolvedores em relação à privacidade de dados, incluindo suas crenças, valores e respostas emocionais; e (iii) *Comportamentos e ações*, que se concentra nos comportamentos e ações reais dos desenvolvedores em relação à privacidade de dados. Ao responder à $QP_1$, torna-se possível identificar os pontos fortes e as lacunas na conscientização dos desenvolvedores sobre a privacidade de dados. Esse entendimento pode contribuir para a criação de programas de treinamento e educação mais eficazes sobre privacidade de dados na indústria de software.

b) **$QP_2$: *Como as percepções dos desenvolvedores sobre frequência, importância e facilidade de uso diferem para várias estratégias de privacidade de dados?*** – $QP_2$ visa compreender as percepções dos desenvolvedores sobre diferentes estratégias de privacidade de dados em termos de frequência de uso, importância e facilidade de uso. Assim, nesta QP, as percepções dos desenvolvedores são comparadas em relação a uma variedade de estratégias (por exemplo, criptografia, anonimização, controle de acesso) para identificar quais estratégias são mais e menos favorecidas pelos desenvolvedores. Ao responder à $QP_2$, busca-se determinar se certas estratégias são subutilizadas devido a desafios percebidos ou supervalorizadas devido à sua importância percebida.

c) **$QP_3$: *Como os fatores organizacionais influenciam a adesão às práticas de privacidade de dados nas equipes de desenvolvimento?*** – A $QP_3$ visa explorar quatro fatores organizacionais: (i) a presença ou não de equipes dedicadas à privacidade; (ii) a dinâmica de trabalho para lidar com a privacidade e a proteção de dados nas organizações; (iii) o uso ou não de ferramentas específicas para gerenciar dados privados; e (iv) as percepções dos participantes sobre a prioridade de sua organização em relação à privacidade e proteção de dados. Ao responder à $QP_3$, busca-se esclarecer como as estruturas organizacionais, prioridades e recursos influenciam a implementação e a adesão às práticas de privacidade de dados nas equipes de desenvolvimento.

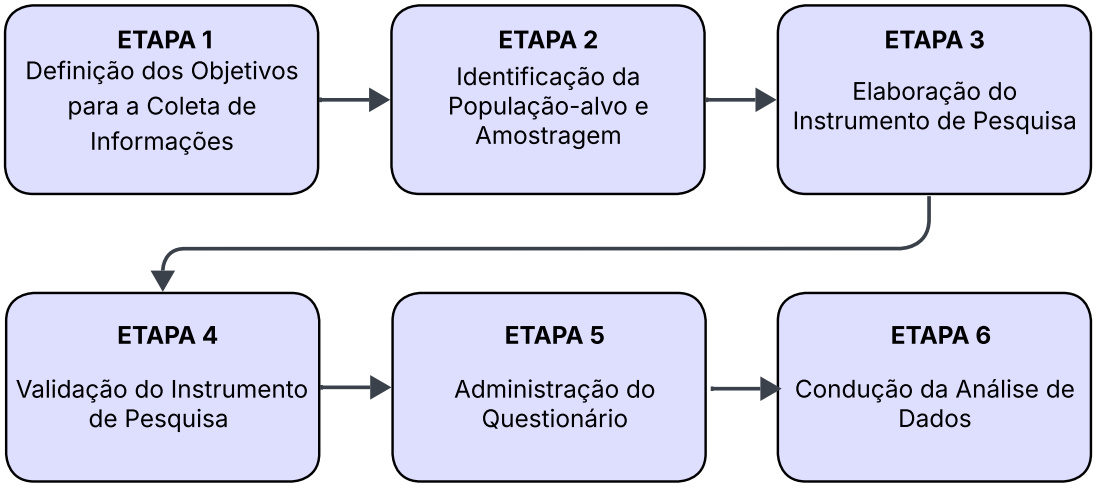
## 4.2 Etapas da Metodologia do Estudo

Para responder às *QPs*, adotou-se o método de pesquisa baseado em questionário ou *survey*. Tal método foi considerado o mais adequado para investigar as *QPs* propostas através de uma amostra relativamente grande de desenvolvedores de software. Para a elaboração e condução do questionário, foram seguidas as diretrizes propostas por Linåker *et al.* (2015) para configurar e conduzir o questionário. A Figura 1 ilustra as principais etapas do estudo. As etapas do processo são descritas em detalhe nas subseções a seguir.

### *4.2.1 Etapa 1: Definição dos Objetivos para a Coleta de Informações*

Nesta etapa, foi conduzida uma sessão de *brainstorming* com o propósito de definir os objetivos e o escopo da pesquisa. O objetivo principal consistiu em avaliar a conscientização dos desenvolvedores acerca da privacidade de dados no contexto do desenvolvimento de software, desde a sua concepção. Ademais, buscou-se examinar

Figura 1 – Etapas e procedimentos metodológicos.




Fonte: Elaborada pela autora (2025).

as práticas associadas à implementação de estratégias de privacidade de dados, bem como a influência de fatores organizacionais sobre a adesão a essas práticas nas equipes de desenvolvimento. Esses objetivos orientaram o *design* e o foco das perguntas do questionário, assegurando a coleta de dados relevantes e abrangentes.

### *4.2.2 Etapa 2: Identificação da População-alvo e Amostragem*

A população-alvo da pesquisa é composta por indivíduos maiores de 18 anos que atuam nas áreas de desenvolvimento de *software* ou segurança da informação no Brasil. Com o intuito de assegurar a adequação do público participante, foi incluída uma questão de controle, que foi utilizada como critério de filtragem (seleção) dos participantes. Essa questão de controle foi destinada a verificar o nível de familiaridade dos respondentes com a temática da privacidade de dados no processo de desenvolvimento de *software*. Adotou-se o procedimento de amostragem do tipo bola de neve (KITCHENHAM; PFLEEGER, 2002), no qual os participantes iniciais indicam e convidam novos participantes, promovendo a expansão iterativa da rede de respondentes.

### *4.2.3 Etapa 3: Elaboração do Instrumento de Pesquisa*

A elaboração do questionário foi realizada de forma colaborativa; o mesmo foi aplicado por meio do *Google Forms*. O questionário consiste em 35 perguntas de diferentes tipos, ou seja, abertas, fechadas, de múltipla escolha e escala Likert. O questionário foi estruturado em cinco seções, conforme apresentado no Quadro 3 e detalhadamente descrito no Apêndice B.

Quadro 3 – Questões do questionário

| ID | Questão | Tipo |
|---|---|---|
| **Caracterização Geral dos Participantes** | | |
| Q1 | Qual é a sua idade? | C |
| Q2 | Em qual estado você reside atualmente? | C |
| Q3 | Qual é o seu gênero? | C |
| Q4 | Qual é o seu nível de educação formal concluída? | C |
| Q5 | Qual é o seu modelo de trabalho? | C |
| Q6 | Qual papel que melhor descreve suas atividades atuais em projetos de desenvolvimento de *software*? | C |
| Q7 | Por favor, indique a senioridade da posição que ocupa. | C |
| Q8 | Quantos anos de experiência você tem em funções relacionadas ao desenvolvimento de *software* ou TI? | C |
| Q9 | Quais são os sistemas que você trabalha atualmente? | M |
| Q10 | Quais são os domínios dos sistemas que você trabalha atualmente? | M |
| Q11 | Qual o setor da organização para a qual você trabalha atualmente? | C |
| Q12 | Qual o tamanho da empresa para a qual você trabalha atualmente? | C |
| **Caracterização da Experiência com Privacidade de Dados** | | |
| Q13 | Você tem (ou teve) alguma experiência de trabalho relacionada à privacidade no processo de desenvolvimento de *software*? | C |
| Q14 | Por favor, descreva brevemente a sua experiência com privacidade de dados em *software*. Em caso negativo, responda que não possui experiência. | O |
| Q15 | Quais são as principais fontes ou métodos que você costuma usar para aprender sobre questões de privacidade relacionadas ao *software*? | M |
| Q16 | Que tipos de dados pessoais você trata no seu trabalho? | M |
| **Conscientização sobre Privacidade de Dados** | | |

*Continua.*

*Continuação.*

| ID | Questão | Tipo |
|---|---|---|
| Q17 | [T1: Conhecimento] Forneça abaixo pelo menos cinco palavras na ordem em que lhe vierem à mente quando você pensa em privacidade. | O |
| Q18 | [T1: Conhecimento] Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco ponto. | L |
| Q19 | [T1: Conhecimento] Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação. (opcional). | O |
| Q20 | [T2: Atitudes e Sentimentos] Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco ponto. | L |
| Q21 | [T2: Atitudes e Sentimentos] Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação. (opcional). | O |
| Q22 | [T3: Comportamentos e Ações] Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco pontos. | L |
| Q23 | [T3: Comportamentos e Ações] Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação (opcional). | O |
| **Estratégias de Implementação de Privacidade de Dados** | | |
| Q24 | Com que frequência você utiliza técnicas e estratégias de privacidade para garantir a proteção de dados pessoais nas seguintes fases de desenvolvimento? | L |
| Q25 | Com que frequência você utiliza ou já utilizou as seguintes estratégias de privacidade? | L |
| Q26 | Você utiliza alguma estratégia de privacidade por design que não foi citada na questão anterior, se sim, qual? (opcional) | O |
| Q27 | Na sua opinião, qual o nível de importância das seguintes estratégias de implementação de privacidade? | L |
| Q28 | Para aquelas estratégias no qual você considerou importante, por favor descreva o motivo da sua classificação (opcional). | O |
| Q29 | Ainda sobre as estratégias, como você caracteriza o grau de facilidade ao usá-las? | L |
| **Fatores Organizacionais** | | |
| Q30 | Em sua organização, existe uma equipe dedicada apenas para lidar com privacidade? | C |
| Q31 | Na sua organização qual a dinâmica de trabalho para lidar com privacidade e proteção de dados? Por favor, descreva brevemente sobre | O |
| Q32 | Na sua organização é utilizado uma ou mais ferramentas como *softwares* para lidar com dados privados? Se sim, quais? | M |
| Q33 | Qual a sua percepção com relação a prioridade da organização em que você trabalha sobre privacidade e proteção de dados? | L |
| Q34 | Na sua percepção quais são os maiores desafios das organizações nos próximos anos sobre práticas e regulamentações para proteger melhor os direitos de privacidade dos usuários? | O |
| Q35 | Por favor, insira o ano atual para mostrar que você não é um bot. | O |

*Continua.*

*Continuação.*

| ID | Questão | Tipo |
|---|---|---|

**Nota.** C: Fechada; M: Múltipla; O: Aberta; L: Likert.

**Fonte:** Elaborado pela autora (2025).

As perguntas foram organizadas e agrupadas intencionalmente de modo a minimizar vieses e evitar a influência entre as respostas dos participantes. Cada seção foi disponibilizada apenas após o preenchimento completo da seção anterior.

No início do questionário, foram disponibilizadas informações gerais sobre o estudo, incluindo seu objetivo, a metodologia empregada, os procedimentos de tratamento de dados e os contatos dos pesquisadores responsáveis. Também foi apresentado um Termo de Consentimento Livre e Esclarecido (TCLE) (ver Apêndice A), descrevendo as condições e estipulações que regiam a participação dos respondentes.[1] Os participantes foram informados de que sua participação era totalmente voluntária e que tinham a liberdade de recusar a participação ou retirar seu consentimento a qualquer momento, sem sofrer qualquer tipo de penalidade. O questionário foi conduzido de forma anônima, sem solicitação de informações de contato dos respondentes.

A primeira seção é composta por perguntas gerais destinadas a coletar informações sobre a formação e as habilidades dos desenvolvedores, definidas por um conjunto de 12 questões. A segunda seção consiste em quatro perguntas voltadas à coleta de dados sobre a experiência do desenvolvedor no trabalho com privacidade de dados em *software*. A terceira seção inclui sete perguntas destinadas a avaliar a conscientização dos desenvolvedores em relação à privacidade de dados ao longo do processo de desenvolvimento de *software*.

Para construir esta seção, baseamo-nos no modelo *Knowledge-Attitude-Behaviour* (KAB) da psicologia social, que fornece um arcabouço para interpretar aspectos pessoais dos desenvolvedores. O modelo KAB tem sido amplamente adotado

[1] As condições estavam em conformidade com os padrões éticos de privacidade previstos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

para estudar a conscientização sobre segurança da informação (por exemplo, (THOMSON; SOLMS, 1998; KRUGER; KEARNEY, 2006; PARSONS *et al.*, 2014)). De forma resumida, conhecimento refere-se a todas as informações que uma pessoa possui ou acumula em um domínio específico (SCHRADER; LAWLESS, 2004). Atitude é composta por três componentes (SCHRADER; LAWLESS, 2004): um componente cognitivo, como uma crença ou ideia associada a um objeto psicológico; um componente afetivo, relacionado à avaliação e emoção do indivíduo em relação a esse objeto; e um componente conativo, que representa predisposições ou ações relativas ao objeto. Neste estudo, o objeto psicológico é a concepção que os participantes têm sobre a privacidade de dados dentro do processo de desenvolvimento de *software*. Por fim, comportamento refere-se a ações observáveis (SCHRADER; LAWLESS, 2004).

Com o modelo KAB em mente, e com base nos achados de estudos anteriores (IWAYA *et al.*, 2023; TAHAEI *et al.*, 2021; HADAR *et al.*, 2018), um conjunto de 21 afirmações foram criadas e categorizadas em três tópicos (T) para capturar diferentes dimensões de conscientização: T1 - *Conhecimento* (com sete afirmações), T2 - *Atitudes e Sentimentos* (com oito afirmações) e T3 - *Comportamentos e Ações* (com seis afirmações). Os participantes foram convidados a avaliar as afirmações com base em sua experiência de trabalho e opiniões, utilizando uma escala Likert de 5 pontos (LIKERT, 1932), variando de *Discordo Fortemente* a *Concordo Fortemente*. Além de atribuir notas às afirmações, os participantes foram estimulados a fornecer uma justificativa para qualquer afirmação com a qual discordassem fortemente em cada tópico.

A quarta seção inclui seis perguntas elaboradas para caracterizar o uso de 13 estratégias de privacidade de dados (por exemplo, criptografia, minimização da coleta de dados pessoais e uso de *proxy*), com foco na frequência de uso, nível de importância e facilidade de uso. Por fim, a quinta seção é composta por cinco perguntas destinadas a identificar fatores organizacionais que podem influenciar a adesão às práticas de privacidade de dados. Também foi incluída uma pergunta adicional para verificar se o

participante era ou não um bot.

### *4.2.4 Etapa 4: Validação do Instrumento de Pesquisa*

Antes da aplicação do questionário, foi conduzido um teste piloto (LITWIN; FINK, 1995) com quatro estudantes de doutorado em Ciência da Computação que não estavam envolvidos em nosso estudo. O *feedback* fornecido pelos participantes contribuiu para o refinamento do instrumento, resultando em ajustes na formulação das perguntas, na inclusão de novas opções de resposta e na reordenação de alternativas em questões fechadas. As recomendações foram incorporadas ao questionário. Vale destacar que as respostas coletadas no teste piloto não foram incluídas nos resultados apresentados neste estudo. Com relação ao tempo de preenchimento, os respondentes do piloto levaram, em média, 15 minutos para concluir o questionário. Esse tempo médio foi informado aos participantes quando o questionário foi disponibilizado publicamente.

### *4.2.5 Etapa 5: Administração do Questionário*

O questionário foi hospedado e administrado na plataforma *Google Forms*. A divulgação do questionário ocorreu por meio de publicações em redes sociais e do envio de mensagens diretas, com o objetivo de alcançar o público-alvo definido. As publicações foram realizadas na *LinkedIn*, enquanto os convites diretos foram encaminhados por LinkedIn, WhatsApp e e-mail. O questionário ficou disponível por 132 dias, de 25 de junho a 5 de novembro de 2024.

### *4.2.6 Etapa 6: Condução da Análise de Dados*

No total, foram obtidas 122 respostas, das quais 34 foram excluídas, com base na questão de controle, por não apresentarem qualquer experiência profissional, direta ou indireta, relacionada à privacidade de dados (mais detalhes para a categorização

do participante podem ser vistos no segundo tópico de discussão da Seção 4.2.6.1). Assim, foram consideradas 88 respostas para análise. Em nossa amostra de dados, cerca de 63,3% dos participantes têm experiência profissional direta relacionada à privacidade de dados, enquanto 38,6% têm experiência indireta. A abordagem de análise variou de acordo com os tipos de perguntas. Para perguntas fechadas e de múltipla escolha, foram calculadas e apresentadas as porcentagens correspondentes a cada opção selecionada, complementadas por visualizações de dados. Para as perguntas da escala *Likert*, foram realizadas análises de correlação. Por fim, para as perguntas abertas, aplicaram-se procedimentos da *Grounded Theory* (GT), com a realização de codificação aberta e axial (CORBIN; STRAUSS, 2008). GT refere-se a um método de geração indutiva de teoria a partir de dados. Os estudos geralmente incluem textos não estruturados, por exemplo, transcrições de entrevistas e notas de campo (GLASER; STRAUSS, 2017).

A seguir, são apresentadas as análises conduzidas para responder às questões de pesquisa (*QPs*) formuladas.

#### *4.2.6.1 Análise para Responder à QP1*

Para abordar a $QP_1$, foram conduzidas análises quantitativas e qualitativas, descritas em detalhe nas subseções a seguir.

**As palavras mais frequentes que os desenvolvedores associam à privacidade de dados.** Para capturar as palavras que os desenvolvedores associam à privacidade de dados, os participantes foram solicitados a listar pelo menos cinco palavras na ordem em que lhes vinham à mente quando pensavam em privacidade (Q17). Nesse contexto, cada palavra foi registrada junto com sua posição na sequência, refletindo a ordem de menção (da 1ª à 5ª palavra). A análise se concentrou em identificar as palavras mais mencionadas em geral e examinar como a ordem de menção influencia sua importância percebida. Nesse contexto, as palavras mencionadas na primeira posição geralmente refletem associações imediatas e centrais, enquanto as listadas posteriormente podem in-

dicar pensamentos complementares ou mais reflexivos. A análise fornece considerações sobre os modelos mentais dos desenvolvedores sobre privacidade de dados, destacando os conceitos-chave e as prioridades que eles associam a esse tópico. A distribuição de frequência das palavras é mostrada na Figura 9.

**Análise de correlações sobre a conscientização sobre privacidade de dados entre diferentes grupos.** Para obter *insights* mais profundos sobre a conscientização dos participantes sobre privacidade de dados, os respondentes foram divididos em diferentes grupos demográficos. Depois, procedeu-se à comparação das respostas obtidas na escala *Likert* obtidas em cada afirmação das perguntas Q18, Q20 e Q23. Foram definidos os seguintes grupos de análise: (a) Respondentes com experiência direta em privacidade de dados (54 respondentes); (b) Respondentes com experiência indireta em privacidade de dados, ou seja, seus grupos realizaram trabalhos relacionados à privacidade de dados, mas os respondentes não estiveram diretamente envolvidos (34 respondentes); (c) Respondentes que trabalham em organizações relativamente maiores (56 respostas); e (d) Respondentes que trabalham em organizações relativamente menores (25 respostas); (e) Respondentes que têm uma função relacionada à privacidade (14 respostas); e (f) Respondentes que não têm uma função relacionada à privacidade (74 respostas).

Para categorizar os participantes com base em sua experiência direta ou indireta com privacidade de dados, foram consideradas as respostas à Pergunta 13, na qual os desenvolvedores indicaram uma das seguintes opções: *Experiência direta*: "Já trabalhei (ou trabalho atualmente) com privacidade de dados no processo de desenvolvimento de *software* (por exemplo, design, desenvolvimento e testes)." *Experiência indireta*: "Meu grupo/equipe de desenvolvimento trabalha (ou já trabalhou) com privacidade, mas não estou diretamente envolvido em nenhuma tarefa."; e *Sem experiência*: "Nunca tive experiência direta ou indireta com privacidade de dados em *software*.". Em relação ao tamanho da organização, a categorização baseou-se nas respostas à Pergunta 12: "Qual é o tamanho da empresa em que você trabalha atualmente?" Com base nas respostas,

as organizações são categorizadas da seguinte forma: *Pequenas organizações*: até 9 funcionários, 10 a 49 funcionários e 50 a 99 funcionários; e *Grandes organizações*: 100 a 499 funcionários, 500 a 999 funcionários e mais de 1.000 funcionários. Por fim, foram consideradas as funções relacionadas à privacidade (Q6), quando os participantes selecionaram uma dessas funções nos projetos de desenvolvimento de *software*: criptógrafo, engenheiro de privacidade, *penetration tester* e engenheiro de segurança.

Para realizar esta análise, foram utilizados o *Wilcoxon Rank Sum Test* (WHITLEY; BALL, 2002) e o *Cliff's Delta* (d) (GRISSOM; KIM, 2005) para determinar o nível de concordância com cada afirmação entre os grupos previamente definidos. A medida *Cliff's Delta* (d) (GRISSOM; KIM, 2005) quantifica a força da diferença entre os grupos. Por exemplo, quão forte é a diferença entre desenvolvedores com experiência direta em privacidade de dados e aqueles com experiência indireta para a afirmação **[S1]**. Utilizamos valores *p* para testar se as diferenças observadas entre os dois grupos eram estatisticamente significativas em um nível de confiança de 95% (valor $p < 0{,}05$). Para interpretar o tamanho do efeito *Cliff's Delta* (d), foi utilizada uma classificação bem conhecida (ROMANO *et al.*, 2006), que define quatro categorias de magnitude, representadas na Tabela 1: insignificante (sem símbolo), pequena (*), média (**) e grande (***). As magnitudes (d) positivas são representadas pelo símbolo (+) e as negativas pelo símbolo ($-$).

Para ilustrar a interpretação da medida (d), a Tabela 1 fornece o seguinte exemplo: para a afirmação **[S18]**, os desenvolvedores com experiência direta em privacidade de dados obtiveram uma média de 4,19, enquanto aqueles com experiência indireta obtiveram uma média de 3,76. O valor *p* associado é 0,05, indicando significância estatística. O *Cliff's Delta* (d) calculado é 0,2015, positivo e classificado como pequeno de acordo com as categorias de magnitude (ROMANO *et al.*, 2006). Em outras palavras, essa interpretação indica que os desenvolvedores com experiência direta concordam mais fortemente com a afirmação **[S18]** em comparação com aqueles com experiência indireta.

**Análise qualitativa.** Foram aplicados procedimentos da GT para analisar as respostas às perguntas abertas (P19, P21, P23), nas quais os participantes descreveram opcionalmente seu desacordo com quaisquer afirmações em análise.

#### *4.2.6.2 Análise para Responder à QP2*

Semelhante à questão anterior, para responder à $QP_2$, foram realizadas análises quantitativas e qualitativas, descritas em detalhe nas subseções a seguir.

**Frequência de uso de estratégias de privacidade de dados nas fases de desenvolvimento.** Os participantes foram solicitados a indicar com que frequência aplicavam estratégias de privacidade em fases específicas do ciclo de vida do desenvolvimento de *software* (Q24). As opções de resposta variavam de "Nunca" a "Sempre", capturando variações na frequência. As fases de desenvolvimento consideradas incluíram Análise de Requisitos, *Design*, Codificação, Estudo de Viabilidade, Instalação, Implantação, Testes e Manutenção. A análise envolveu as seguintes etapas: (1) As respostas foram categorizadas por nível de frequência ("Nunca", "Raramente", "Às vezes", "Frequentemente", "Sempre") para cada fase de desenvolvimento. Essa etapa permitiu uma compreensão clara de como as estratégias de privacidade foram distribuídas ao longo do ciclo de vida e (2) em seguida, foi calculada a proporção de participantes que selecionaram cada nível de frequência para cada fase de desenvolvimento. Isso permitiu identificar as fases em que as estratégias de privacidade foram mais e menos utilizadas.

**Análise de correlações sobre as percepções de frequência, importância percebida e facilidade de uso das estratégias de privacidade de dados.** Para avaliar as percepções dos desenvolvedores sobre as estratégias de privacidade de dados, analisamos os dados sobre a frequência de uso (Q25), importância percebida (Q27) e facilidade de uso (Q29) de 13 estratégias, com base nas respostas de 88 desenvolvedores. Nesse contexto, para considerar os diferentes níveis de especialização entre os desenvolvedores, adaptamos uma metodologia inspirada em um estudo anterior (DIAS-NETO *et al.*, 2017).

Essa abordagem envolveu três etapas principais, detalhadas a seguir:

*Etapa 1 - Atribuição de peso:* A cada participante foi atribuído um peso com base em seus anos de experiência, nível de senioridade, grau acadêmico e a relação entre experiência direta e especialização em privacidade de dados (Eq.4.1). O peso atribuído reflete a especialização geral do participante, considerando tanto as qualificações formais quanto a experiência prática.

$$W(i) = E(i) + S(i) + \left(\frac{Y(i)}{\text{Mediana}(Y)}\right) + R(i), \text{onde:} \tag{4.1}$$

a) $W(i)$: é o peso total atribuído ao participante $i$;

b) $E(i)$: é o nível acadêmico mais alto do participante $i$, como (1) Ensino Médio, (2) Bacharelado, (3) Especialização, (4) Estudante de Mestrado, (5) Mestrado, (6) Estudante de Doutorado e (7) Doutorado;

c) $S(i)$: é o nível de senioridade relatado pelo participante $i$ em sua posição atual, como (1) Estagiário/*Trainee*, (2) Júnior (até 5 anos), (3) Pleno (6 a 9 anos) e (4) Sênior (mais de 10 anos);

d) $Y(i)$: é o número de anos de experiência relatado pelo participante $i$ em desenvolvimento de *software*, como (1) Menos de 1 ano, (2) Entre 1 e 3 anos, (3) Entre 4 e 6 anos, (4) Entre 7 e 14 anos e (5) Mais de 15 anos;

e) Mediana$(Y)$: é a mediana dos anos de experiência em desenvolvimento, considerando as respostas de todos os participantes; e

f) $R(i)$: representa o valor da relação entre experiência direta e especialização em privacidade de dados.

Explicamos o $R(i)$ da seguinte forma (Eq. 4.2).

$$R(i) = \frac{D(i) + X(i)}{2}, \text{onde:} \tag{4.2}$$

a) $R(i)$: é o valor da relação entre experiência direta e especialização em privacidade de dados;

b) $D(i)$: indica experiência direta em privacidade de dados, com um valor de 1 se o desenvolvedor tiver experiência direta em privacidade de dados, caso contrário, 0;

c) $X(i)$: denota a experiência do desenvolvedor em privacidade de dados, atribuindo um valor de 1 se o desenvolvedor for um especialista em privacidade de dados, ou seja, se sua posição atual for criptógrafo, engenheiro de privacidade, *penetration tester* ou engenheiro de segurança, caso contrário, 0.

Em resumo, $R(i)$ calcula a média de dois atributos binários, $D(i)$ e $X(i)$, para refletir a relação geral do participante entre experiência direta e especialização profissional em privacidade de dados. A interpretação para cada caso é a seguinte:

a) $D = 0, X = 0$: O participante não tem experiência direta nem conhecimento profissional em privacidade de dados. Neste caso, $R = 0$, indicando nenhuma relação;

b) $D = 1, X = 0$: O participante tem experiência direta, mas não é considerado um especialista. Aqui, $R = 0,5$, representa um envolvimento moderado.

c) $D = 0, X = 1$: O participante é considerado um especialista, mas não tem experiência direta. Da mesma forma, $R = 0,5$.

d) $D = 1, X = 1$: O participante possui experiência direta e conhecimento profissional em privacidade de dados. Neste caso, $R = 1$, indicando o mais alto nível de relevância.

*Etapa 2 - Respostas ponderadas:* Após atribuir pesos, a resposta de cada participante à frequência de uso, importância percebida e facilidade de uso das 13 estratégias foi multiplicada pelo peso correspondente. Isso resulta em uma pontuação ponderada para cada estratégia. O valor total para cada estratégia é então calculado somando-se essas respostas ponderadas de todos os participantes, conforme definido na

Eq. 4.3.

$$T(j) = \sum_{i=1}^{n} (\text{Resposta(i, j)} \times \text{W(i)}), \text{onde:} \tag{4.3}$$

a) $T(j)$: é o valor total da frequência de uso, importância percebida e facilidade de uso para a estratégia de privacidade de dados $j$;

b) $Resposta(i, j)$: é o valor da resposta que varia de 1 a 5, relacionado à frequência de uso, importância percebida e facilidade de uso do participante $i$ na estratégia de privacidade de dados $j$;

c) $W(i)$: é o peso para o participante $i$.

*Etapa 3 - Normalização:* Por fim, foi calculado um valor normalizado para os níveis de uso, importância percebida e facilidade de uso, variando de 0 a 100%, normalizando o valor obtido na Etapa 2 para cada estratégia de privacidade de dados, ou seja, dividindo o valor alcançado na etapa anterior pelo valor máximo possível (conforme definido na Eq. 4.4).

$$N(j) = \frac{T(j)}{\sum_{i=1}^{n} (\text{W(i)}) \times PontMaxPorParticipante}, \text{onde:} \tag{4.4}$$

a) $N(j)$: é o valor normalizado para a frequência de uso ou importância percebida ou facilidade de uso de uma estratégia de privacidade de dados $j$;

b) $T(j)$: é o valor total calculado para a estratégia $j$ na Etapa 2;

c) $W(i)$: é o valor de peso para o participante $i$;

d) $PontMaxPorParticipante$: é a pontuação máxima que um participante pode fornecer (por exemplo, em uma escala Likert de 5 pontos).

O valor normalizado (Eq.4.4) é usado na Tabela 3 para comparar a frequência de uso, a importância percebida e a facilidade de uso de cada estratégia de privacidade

de dados. Para demonstrar a aplicação da fórmula, usamos as respostas de importância percebida para a estratégia de criptografia (Tabela 3) como exemplo, da seguinte forma:

*Calcule o valor total de importância percebida:* A importância total percebida ($T$) para esta estratégia é calculada multiplicando o peso de cada desenvolvedor ($W(i)$) pela resposta correspondente ($Resposta(i, Criptografia)$) e somando os resultados de todos os participantes ($n$). Neste caso, ($T(\text{Criptografia})) \approx 1136{,}98$:

$$T(\text{Criptografia}) = \sum_{i=1}^{n} (\text{Resposta(i, Criptografia)} \times \text{W(i)})$$

*Normalizar para determinar o nível de importância percebido:* O nível de importância percebido é determinado como uma porcentagem, variando de 0% a 100%, normalizando o valor total de importância. Isso é feito dividindo $T(Criptografia)$ pela soma dos pesos possíveis para todos os participantes $\sum_{i=1}^{n}(\text{W(i)})$, multiplicada por 5. A normalização garante que os resultados sejam comparáveis entre todas as estratégias, independentemente do número de participantes ou de seus pesos.

$$N(j) = \frac{1136,98}{241,85 \times 5} \approx 0,940$$

O resultado, $N(j) \approx$ 0,940, indica que a importância percebida da estratégia de Criptografia é de aproximadamente 94,02%.

**Análise qualitativa.** Foram igualmente aplicados procedimentos da GT para a análise das respostas às perguntas abertas (P26 e P28), ambas opcionais. Na P26, perguntou-se aos participantes se eles usavam alguma estratégia de implementação adicional para garantir a privacidade além das mencionadas na pergunta anterior (P25) e, em caso afirmativo, que as especificassem. Essa pergunta tinha como objetivo revelar estratégias únicas ou menos convencionais que pudessem complementar ou expandir o conjunto predefinido de estratégias. Para a Q28, os participantes forneceram explicações

para classificar certas estratégias como importantes. Essas respostas adicionaram profundidade e contexto, esclarecendo os processos de tomada de decisão dos participantes, suas prioridades e os desafios específicos que enfrentaram na implementação de estratégias de privacidade.

#### *4.2.6.3 Análise para Responder à QP3*

Para abordar a $QP_3$, foram conduzidas análises qualitativas e quantitativas para descobrir como as organizações gerenciam a privacidade e a proteção de dados e a influência dos fatores organizacionais na adoção de estratégias de privacidade.

**Análise qualitativa.** Foram analisadas as respostas a duas perguntas abertas (Q31 e Q34), nas quais 88 participantes descreveram as práticas de suas organizações para gerenciar a privacidade e a proteção de dados, bem como sua percepção dos desafios futuros para as organizações na proteção dos direitos de privacidade dos usuários. Por meio dessa análise, foram identificadas nove categorias distintas de práticas relacionadas ao gerenciamento da privacidade e oito categorias de desafios. As descobertas foram posteriormente comparadas com resultados de estudos anteriores, com o propósito de contextualizar e validar as evidências obtidas. **Análise quantitativa.** Foram examinadas como as estruturas organizacionais influenciam a adoção de estratégias de privacidade. Nossa análise se concentrou em três aspectos principais: (1) a presença de equipes dedicadas à privacidade (Q30); (2) adoção de ferramentas e padrões de uso (Q32); e (3) prioridade organizacional percebida (Q33).

## 4.3 Resumo do Capítulo 4

Esta pesquisa adota uma análise quantitativa e qualitativa, de caráter descritivo e exploratório, buscando compreender como desenvolvedores de *software* percebem e aplicam estratégias de privacidade de dados em seus projetos. O estudo foi realizado

por meio de um *survey* estruturado aplicado a desenvolvedores de *software* e analistas de segurança da informação, com o objetivo de coletar dados acerca de percepção dos desenvolvedores de *software*. Os procedimentos metodológicos apresentados nesta seção estabelecem as bases para a análise dos resultados, discutidos no Capítulo 5.

# 5 RESULTADOS

Este capítulo está organizado da seguinte forma: Na Seção 5.1 é apresentado a caracterização geral dos participantes. Em seguida, na Seção 5.2 é discutido os resultados relacionados à conscientização dos desenvolvedores acerca da privacidade de dados. Logo após na Seção 5.3 é abordado as estratégias de privacidade utilizadas pelos desenvolvedores. Por fim, na Seção 5.4 é analisado a influência de fatores organizacionais na adoção do uso de estratégias de privacidade de dados.

Como mencionado na Seção 4.2.6, a amostra de dados deste estudo consistiu em 88 respostas para análise. Consideramos apenas os participantes que relataram experiência de trabalho direta ou indireta relacionada à privacidade de dados. Para simplificar, utilizaremos a notação (*n*/88) ao longo do texto para indicar um número *n* dentre os 88 participantes válidos.

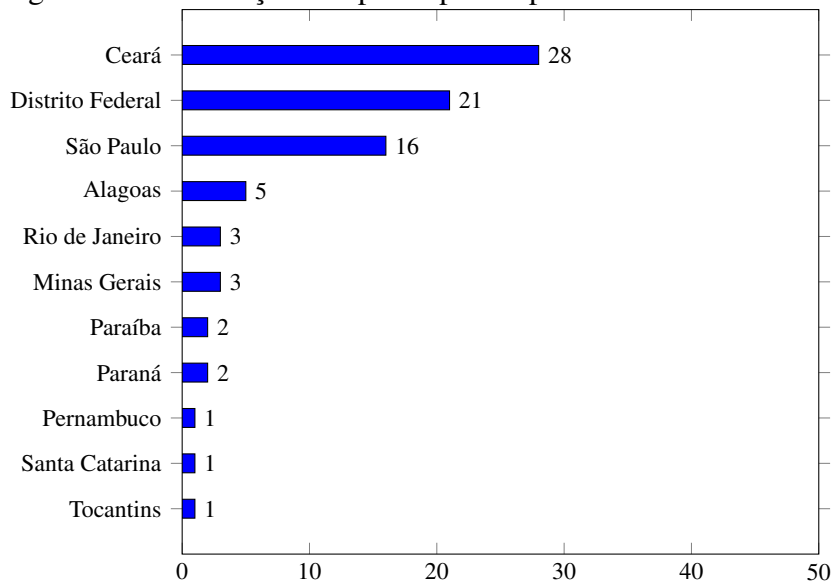
## 5.1 Caracterização Geral dos Participantes

A Figura 2 fornece uma visão geral da distribuição dos participantes por estados brasileiros (Q2).

Os participantes estão distribuídos em 11 estados brasileiros (Q2), com predominância significativa no Ceará (28 participantes, representando 35% do total), seguido pelo Distrito Federal (21 participantes, 2%) e São Paulo (16 participantes, 20%). Outros estados com menor representação incluem Alagoas (5 participantes), Rio de Janeiro (3 participantes), Minas Gerais (3 participantes), Paraíba (2 participantes), Paraná (2 participantes), além de Pernambuco, Santa Catarina e Tocantins (1 participante cada). Essa distribuição reflete uma concentração regional no Nordeste e Centro-Oeste, com representação notável do Sudeste.

Os participantes são predominantemente homens (Q3), representando 85,2% (75/88) da amostra, enquanto apenas 14,8% (13/88) são mulheres, uma tendência co-

Figura 2 – Distribuição dos participantes por estados brasileiros




Fonte: Elaborada pela autora (2025).

mumente observada em áreas relacionadas à tecnologia (ASHCRAFT *et al.*, 2016). Em relação à idade (Q1), a maioria dos participantes está na faixa de 25 a 34 anos, correspondendo a 44,3% (39/88), seguida pelo grupo de 35 a 44 anos, com 25% (22/88). Já 20,5% (18/88) têm entre 18 e 24 anos, e um participante (1,1%) está na faixa de 55 a 64 anos. Além disso, um participante (1,1%) preferiu não informar a idade. Quanto à formação acadêmica (Q4), a maioria possui pelo menos graduação completa, sendo que 29,5% (26/88) têm diploma de bacharelado. Além disso, 19,3% (17/88) concluíram uma especialização, enquanto 13,6% (12/88) possuem apenas o ensino médio. Aproximadamente 20% têm ou estão cursando pós-graduação: 11,4% (10/88) são estudantes de mestrado, 10,2% (9/88) têm doutorado e outros 10,2% (9/88) já concluíram o mestrado. Por fim, 5,7% (5/88) são doutorandos. Esses dados indicam que a amostra possui um perfil altamente acadêmico.

Foi solicitado aos participantes que informassem seu modelo de trabalho atual (Q5). Observou-se que a maioria, 62,5% (55/88), trabalha de forma remota, refletindo uma tendência comum na indústria de tecnologia, especialmente no período

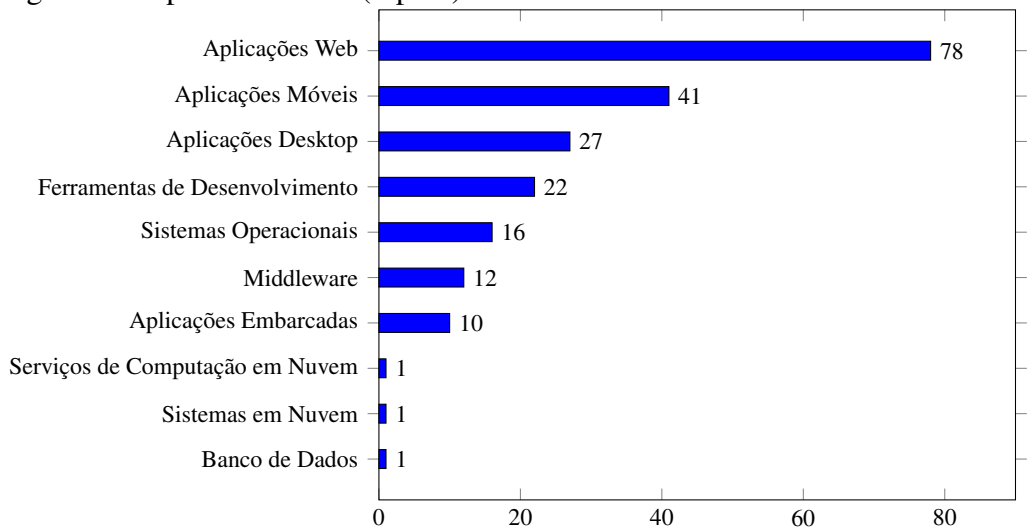
pós-pandemia (RALPH *et al.*, 2020). Já os modelos híbridos (18,2%, 16/88) e presenciais (19,3%, 17/88) são menos frequentes, mas ainda assim representam uma parcela considerável da amostra (cerca de 37%). Além disso, a maioria dos participantes exerce funções tradicionais dentro de projetos de desenvolvimento de *software* (Q6). Em especial, 50,6% (44/88) são desenvolvedores (incluindo *backend*, *frontend* e *fullstack*), e 10,3% (9/88) atuam como engenheiros de segurança. Outras funções incluem líderes de projeto e cientistas de dados (5,7%, 5/88 cada). Também aparecem gerentes ou testadores, arquitetos de soluções e engenheiros de privacidade, cada um representando 3,4% (3/88), seguidos por *product owners* e *pentester*, com 2,3% (2/88) cada. Outras funções, como engenheiros de dados, *designers* UX/UI, administradores de banco de dados e auditores de TI, também aparecem, cada uma com 1,1% (1/88). Esses dados sugerem que a maior parte dos participantes atua diretamente em funções de desenvolvimento.

A maioria dos participantes é sênior (Q7), com 39,8% (35/88) possuindo pelo menos 10 anos de experiência ou mais em suas áreas, e 33% (29/88) classificados como nível pleno, ou seja, com 6 a 9 anos de experiência. Em contraste, 21,6% (19/88) são juniores (com até 5 anos de experiência) e 5,7% (5/88) ocupam posições de estagiário/trainee. Essa distribuição indica uma amostra bastante experiente, com quase 40% dos participantes em cargos sênior, refletindo a profundidade de conhecimento da amostra. Em relação aos anos de experiência em desenvolvimento de *software* (Q8), a maioria dos participantes apresenta alto nível de experiência: 34,1% (30/88) têm entre 7 e 14 anos, e 19,3% (17/88) têm mais de 15 anos. Além disso, 26,1% (23/88) possuem entre 4 e 6 anos, 13,6% (12/88) entre 1 e 3 anos, e 6,8% (6/88) menos de 1 ano de experiência, o que garante alguma diversidade no histórico profissional.

Os participantes também foram questionados sobre o tipo de sistemas com os quais trabalham (Q9) e os respectivos domínios desses sistemas (Q10). Essas foram questões de múltipla escolha, permitindo que os participantes selecionassem várias opções. A Figura 3 mostra que o tipo mais comum de sistema foi aplicações *web* (78),

seguido por aplicações móveis (41) e aplicações *desktop* (27). Outros tipos incluíram ferramentas de desenvolvimento (22), sistemas operacionais (16), *middleware* (12) e aplicações embarcadas (10).

Figura 3 – Tipo de sistemas (top 10)



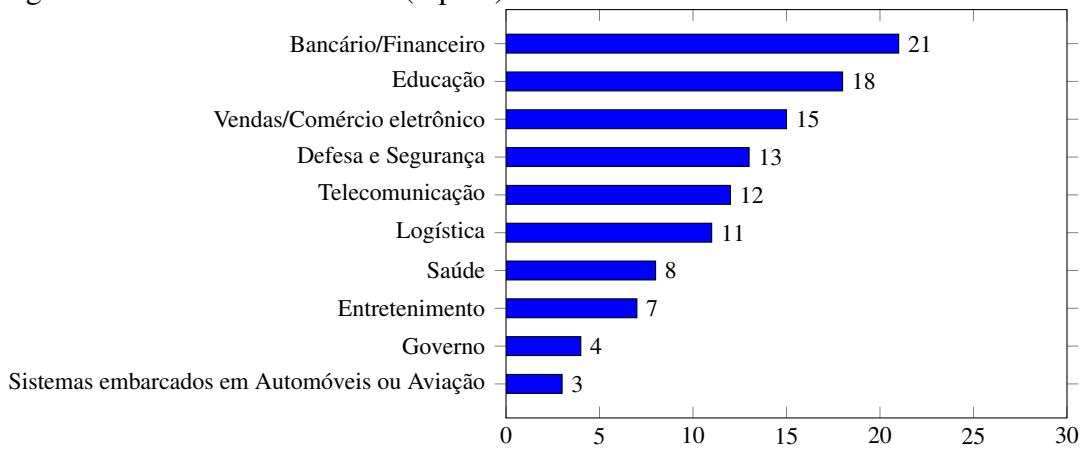

Fonte: Elaborada pela autora (2025).

A Figura 4 mostra que o domínio do sistema mais comum foi o bancário/-financeiro (21), seguido por educação (18), vendas/comércio eletrônico (15), defesa e segurança (13), telecomunicações (12), entre outros.

**Caracterização das organizações.** Os participantes foram questionados sobre o porte (Q12) e o setor de atuação (Q11) das organizações em que trabalham. Figura 5 mostra que a maioria dos participantes atua em grandes organizações com mais de 1000 funcionários (43,1%, 38/88), seguidas por organizações com 100 a 499 funcionários (13,6%, 12/88), 10 a 49 funcionários (12,5%, 12/88), até 9 funcionários (11,3%, 10/88), 500 a 999 funcionários (6,8%, 6/88) e 50 a 99 funcionários (4,5%, 4/88). Apenas sete participantes indicaram não saber o porte da sua organização.

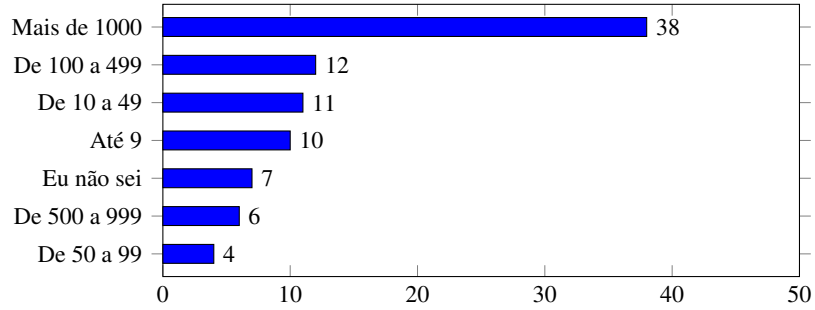
A Figura 6 ilustra que a maioria dos participantes trabalha em organizações privadas (48,8%, 43/88), seguidos por aqueles que atuam na administração pública

Figura 4 – Domínio do sistema (top 10)




Fonte: Elaborada pela autora (2025).

Figura 5 – Tamanho da organização

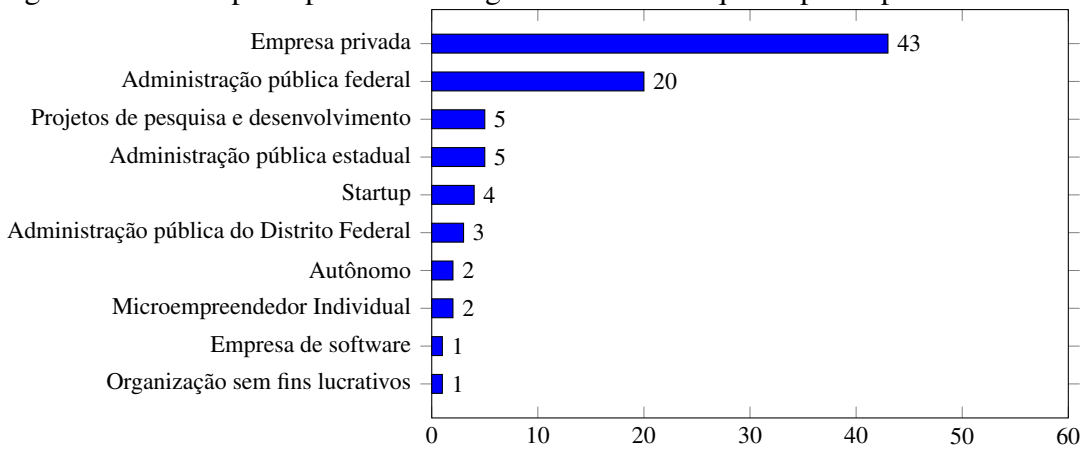



Fonte: Elaborada pela autora (2025).

federal (22,7%, 20/88).

**Experiência específica com privacidade de dados no processo de desenvolvimento.** Os participantes também foram questionados sobre a existência de experiência profissional relacionada à privacidade de dados (Q13). Um total de 61,4% (54/88) dos participantes responderam que já trabalhou (ou atualmente trabalha) com privacidade de dados no processo de desenvolvimento de *software* (por exemplo, *design*, desenvolvimento e testes), enquanto 38,6% (34/88) indicaram ter uma experiência indireta, afirmando que sua equipe trabalha (ou já trabalhou) com privacidade de dados, mas eles não estiveram diretamente envolvidos em nenhuma tarefa. Os participantes relataram sua experiência com privacidade de dados na Q14 (pergunta aberta), por exemplo:

Figura 6 – Os dez principais setores organizacionais em que os participantes trabalham



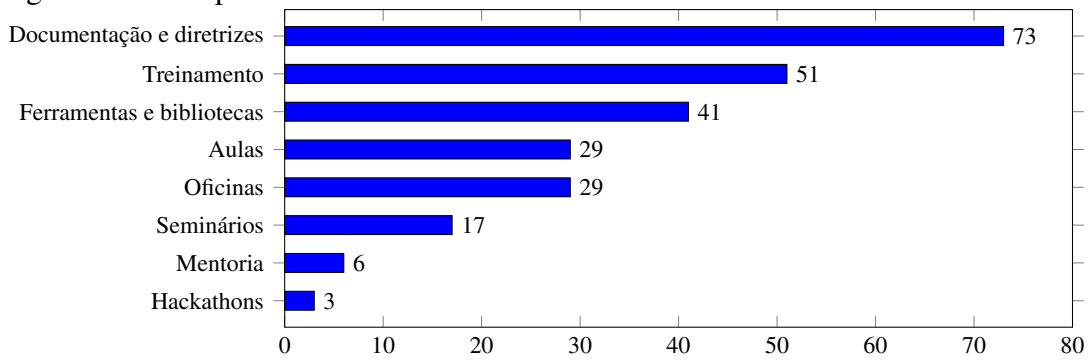

Fonte: Elaborada pela autora (2025).

> *#P79 disse: "Minha experiência com privacidade de dados está relacionada à criticidade das informações financeiras, tanto para transações quanto para os dados pessoais dos clientes. Devemos tratar o uso e compartilhamento desses dados com extremo cuidado para garantir a conformidade com a LGPD e outras leis/regulamentos aplicáveis. Isso envolve processamento de dados, questões de armazenamento, não armazenamento e redirecionamento."*

Os participantes também foram questionados sobre as principais fontes ou métodos utilizados para aprender sobre questões relacionadas à privacidade de dados em *software* (Q15) e sobre quais tipos de dados pessoais eles manipulam em seu trabalho (Q16). Essas foram perguntas de múltipla escolha, permitindo que os participantes selecionassem quantas opções desejassem. Os resultados, resumidos na Figura 7, mostram que as fontes mais comuns incluem documentação e diretrizes (73), seguidas por programas de treinamento (51) e ferramentas e bibliotecas (41). Outras fontes foram palestras (29), workshops (20), seminários (17), mentoria (6) e *hackathons* (3).

A Figura 8 mostra que o tipo de dado mais frequentemente manipulado são os identificadores de contato básicos, com 83 respostas, incluindo informações como

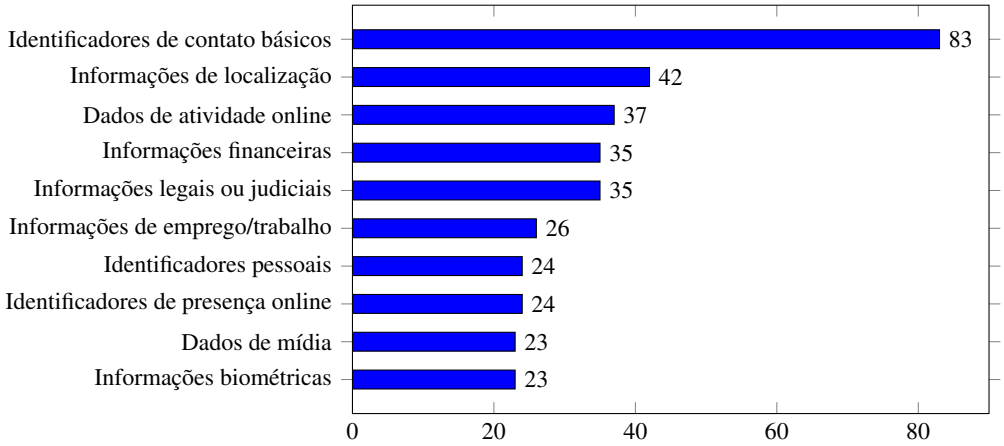
Figura 7 – Principais fontes de conhecimento




Fonte: Elaborada pela autora (2025).

nomes, e-mails, números de telefone e IDs pessoais de usuários. Em seguida vêm as informações de localização (42 respostas), por exemplo, dados de geolocalização, e os dados de atividade online (37 respostas), que incluem logs de sites, endereços IP, user agents e IDs de dispositivos. Outros tipos de dados pessoais incluem informações financeiras e informações legais ou judiciais, ambas com 35 respostas, indicando o manuseio de dados sensíveis relacionados a finanças ou processos legais.

Figura 8 – Os dez principais tipos de dados pessoais tratados pelos participantes




Fonte: Elaborada pela autora (2025).

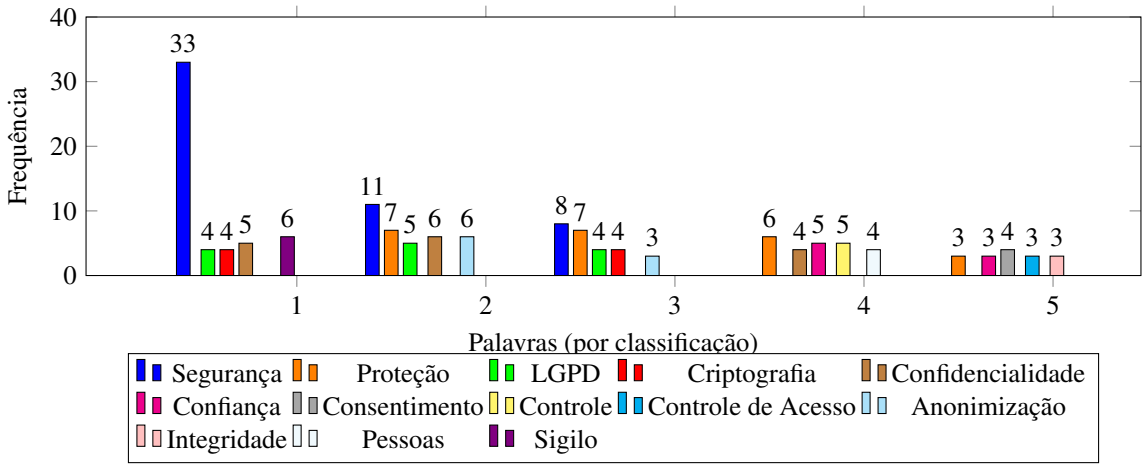
## 5.2 Conscientização dos Desenvolvedores sobre Privacidade de Dados (QP1)

Para responder à $\mathbf{QP}_1$, foram analisados: (i) as palavras mais frequentes que vêm imediatamente à mente dos desenvolvedores quando pensam em privacidade de dados (Q17); e (ii) o nível de concordância dos desenvolvedores com 21 afirmações, considerando diferentes grupos, em três dimensões: *Conhecimento*, que avalia a compreensão dos desenvolvedores sobre princípios, leis e melhores práticas de privacidade de dados (Q18); *Atitudes e Sentimentos*, que explora suas crenças, valores e respostas emocionais em relação à privacidade de dados (Q20); e *Comportamentos e Ações*, que foca nos comportamentos e ações efetivamente adotados pelos desenvolvedores em relação à privacidade de dados (Q22). Os procedimentos de análise de dados empregados para responder à $QP_1$ são detalhados na Seção 4.2.6.1.

**As palavras mais frequentes que os desenvolvedores associam à privacidade de dados.** Foi solicitado aos participantes para *Fornecer pelo menos cinco palavras na ordem em que surgem à mente quando você pensa em privacidade* (Q17). Esta questão teve como objetivo capturar as associações imediatas e os conceitos-chave que os desenvolvedores vinculam à privacidade de dados. A Figura 9 mostra a distribuição de frequência das palavras mais associadas à privacidade de dados pelos participantes. O eixo x representa a posição das palavras na ordem fornecida pelos participantes (de 1 a 5). Esses números correspondem à sequência em que os participantes listaram as palavras.

Figura 9 revela que a palavra *Segurança* aparece com mais frequência nas posições ranking = 1, 2 e 3 com 33, 11 e 8 menções, respectivamente. Isso sugere que segurança é a ideia central e imediata associada à privacidade de dados na mente dos respondentes. No ranking=2, a distribuição das palavras se torna mais variada, com *Proteção* (7 menções), *Confidencialidade* (6 menções), *Anonimização* (6 menções) e *Lei Geral de Proteção de Dados - LGPD* (5 menções). Essas associações indicam que os

Figura 9 – Frequência das 5 palavras mais mencionadas por classificação.




Fonte: Elaborada pela autora (2025).

participantes vinculam a privacidade não apenas a medidas protetivas, mas também a estruturas legais, como as previstas na *LGPD*.

No ranking=3, a frequência das palavras diminui, com *Criptografia* aparecendo pela segunda vez, com quatro menções. Isso indica que as preocupações com privacidade se estendem a questões mais específicas, como estratégias de privacidade de dados, por exemplo, a criptografia. No ranking=4, *Proteção* aparece pela terceira vez com seis menções, seguida por *Confiança* e *Controle* com cinco menções, e *Confidencialidade* e *Pessoas* com quatro menções. Por fim, no ranking=5, Consentimento aparece como a palavra mais mencionada, com quatro menções, seguida por *Proteção*, *Confiança*, *Controle de Acesso* e *Integridade*, cada uma com três menções. Essa progressão reflete uma transição de conceitos mais gerais - como segurança e proteção - para uma combinação de fatores técnicos, legais e interpessoais que desempenham papel na privacidade de dados.

**Achado 1:** Os desenvolvedores frequentemente associam a palavra segurança à privacidade de dados, já que ela ocupou as posições mais altas nos três primeiros rankings fornecidos pelos participantes (33 menções no ranking 1, 11 no ranking 2 e 8 no ranking 3). Isso destaca a segurança como o conceito principal e imediatamente vinculado à privacidade.

**Consciência, perspectivas e práticas dos desenvolvedores.** A Tabela 1 apresenta uma visão geral dos resultados sobre a conscientização em relação às declarações de privacidade de dados, indicando que 12 afirmações apresentaram diferenças estatisticamente significativas entre os grupos. Adicionalmente, foi utilizada uma codificação de cores para indicar qual grupo tinha maior probabilidade de concordar com cada afirmação: a cor cinza escuro indica que o primeiro grupo apresentou maior nível de concordância, enquanto a cor cinza claro indica que o segundo grupo teve maior probabilidade de concordância.

Além disso, cada afirmação foi anotada para indicar diferenças estatisticamente significativas entre grupos, conforme segue: (1) 🔧 indica diferença significativa entre participantes com experiência de trabalho **direta** e aqueles com experiência **indireta** em privacidade de dados; (2) 📱 denota diferença significativa entre os grupos de função **especialista** e **não especialista**; e (3) 👥 indica diferença significativa entre participantes que trabalham em organizações de **grande** e **pequeno** porte.

Por exemplo, **[S1]** mostra que não há diferenças significativas entre nenhum dos grupos de participantes em relação à percepção sobre essa afirmação. Por outro lado, **[👥📱S2]** indica que há uma diferença significativa entre os grupos que atuam em organizações **grandes** e **pequenas**, assim como entre os grupos de **especialistas** e **não especialistas**, quanto à percepção sobre a afirmação S2.

**🔧 Experiência Direta vs. Indireta em Trabalho com Privacidade de Dados.** A experiência direta em privacidade mostrou maior impacto no conhecimento

Tabela 1 – Resultados da pesquisa sobre a conscientização em relação às declarações de privacidade de dados

| Afirmação | ID | Likert | Direta vs. Indireta | | | | Grande vs. Pequena | | | | Especialista vs. Não especialista | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Média | Média | Média | *p-value* | *d* | Média | Média | *p-value* | *d* | Média | Média | *p-value* | *d* |
| **Tópico 1: Conhecimento sobre Privacidade de Dados em *Software*** | | | | | | | | | | | | | | |
| Tenho conhecimento das leis de privacidade relevantes para minha área, como a ISO/IEC 29100 e o conceito de Privacy by Design. | S1 | 3.43 | 3.61 | 3.15 | 0.07 | (+)* | 3.63 | 3.08 | **0.02** | (+)* | 4.29 | 3.17 | **0.00** | (+)*** |
| Tenho uma compreensão sólida das leis e regulamentações de privacidade específicas que se aplicam ao meu trabalho e de como elas influenciam o desenvolvimento de *software*. | S2 | 3.65 | 3.67 | 3.62 | 0.44 | (+) | 3.88 | 3.32 | **0.04** | (+)* | 4.43 | 3.38 | **0.00** | (+)*** |
| Participei de treinamentos internos ou workshops sobre segurança e privacidade, incluindo políticas internas de privacidade e regulamentações específicas do setor. | S3 | 3.56 | 3.59 | 3.50 | 0.35 | (+) | 3.95 | 3.16 | **0.01** | (+)* | 3.93 | 3.40 | 0.08 | (+)* |
| Busco aprender sobre privacidade por iniciativa própria, incluindo a leitura de leis e regulamentações e a consulta a especialistas. | S4 | 3.82 | 3.94 | 3.62 | 0.08 | (+)* | 3.88 | 3.80 | 0.45 | (+) | 4.43 | 3.66 | **0.00** | (+)** |
| Reconheço os riscos e preocupações relacionados à privacidade de dados em sistemas de *software*, como vazamento de dados pessoais, acesso não autorizado e falta de controle sobre dados do usuário. | S5 | 4.57 | 4.57 | 4.56 | 0.51 | (-) | 4.61 | 4.56 | 0.76 | (-) | 4.79 | 4.52 | 0.12 | (+)* |
| Estou ciente das melhores práticas e técnicas para proteger a privacidade do usuário em sistemas de *software*, incluindo anonimização e controle de acesso. | S6 | 3.90 | 3.98 | 3.76 | 0.22 | (+) | 4.00 | 3.76 | 0.11 | (+)* | 4.64 | 3.69 | **0.00** | (+)*** |
| Compreendo a diferença entre segurança e privacidade, reconhecendo que a privacidade vai além da proteção de dados e inclui aspectos como controle e consentimento informado. | S7 | 4.13 | 4.19 | 4.03 | 0.25 | (+) | 4.16 | 4.08 | 0.44 | (+) | 4.29 | 4.05 | **0.04** | (+)* |
| **Tópico 2: Atitudes e Percepções sobre a Privacidade de Dados em *Software*** | | | | | | | | | | | | | | |
| Tenho preocupação com a possibilidade de ser monitorado(a) ou manipulado(a) ao usar aplicativos, redes sociais ou navegar na internet. | S8 | 4.30 | 4.30 | 4.29 | 0.65 | (-) | 4.32 | 4.20 | 0.40 | (+) | 4.71 | 4.25 | **0.02** | (+)* |
| Acredito que a privacidade pessoal é um direito fundamental e que devemos estar atentos a violações de privacidade. | S9 | 4.60 | 4.61 | 4.59 | 0.36 | (+) | 4.55 | 4.68 | 0.89 | (-) | 4.50 | 4.63 | 0.66 | (-) |
| Sinto-me pessoalmente responsável por proteger a privacidade dos usuários em meu trabalho como desenvolvedor(a) de *software*. | S10 | 4.42 | 4.44 | 4.38 | 0.46 | (+) | 4.38 | 4.44 | 0.61 | (-) | 4.64 | 4.42 | 0.20 | (+) |
| Percebo que muitas pessoas não se preocupam com privacidade, mas acredito que ainda é importante educar e conscientizar sobre direitos de privacidade. | S11 | 4.34 | 4.33 | 4.35 | 0.43 | (+) | 4.18 | 4.56 | 0.98 | (-)* | 4.64 | 4.29 | 0.10 | (+)* |
| Sinto-me frustrado(a) com a ideia de que a privacidade é inalcançável na sociedade digital atual. | S12 | 3.58 | 3.48 | 3.74 | 0.86 | (-) | 3.50 | 3.56 | 0.58 | (-) | 3.79 | 3.62 | 0.30 | (+) |
| Valorizo o consentimento informado dos usuários antes da coleta de dados e acredito que ele é essencial para uma relação de confiança entre usuário e desenvolvedor. | S13 | 4.28 | 4.43 | 4.06 | 0.06 | (+)* | 4.14 | 4.48 | 0.95 | (-)* | 4.07 | 4.32 | 0.66 | (-) |
| Reconheço que a retenção de dados pessoais deve ser limitada e depender do tipo de dado e do propósito do sistema. | S14 | 4.58 | 4.54 | 4.65 | 0.68 | (-) | 4.55 | 4.68 | 0.89 | (-) | 4.71 | 4.57 | 0.27 | (+) |
| Considero que a privacidade é uma responsabilidade compartilhada de toda a equipe de desenvolvimento. | S15 | 4.51 | 4.61 | 4.35 | 0.06 | (+)* | 4.45 | 4.60 | 0.89 | (-)* | 4.71 | 4.51 | 0.13 | (+)* |
| **Tópico 3: Comportamentos e Ações em Relação à Privacidade de Dados em *Software*** | | | | | | | | | | | | | | |
| Identificar questões de privacidade durante o desenvolvimento faz parte da minha rotina profissional. | S16 | 3.75 | 3.87 | 3.56 | 0.10 | (+)* | 3.66 | 3.84 | 0.79 | (-) | 4.29 | 3.58 | **0.00** | (+)** |
| Quando encontro problemas de privacidade, encaminho-os a líderes de projeto, colegas mais experientes ou à equipe de segurança. | S17 | 4.28 | 4.31 | 4.24 | 0.41 | (+) | 4.20 | 4.36 | 0.91 | (-)* | 4.43 | 4.22 | 0.18 | (+) |
| Proponho soluções para problemas de privacidade encontrados durante o desenvolvimento de *software*. | S18 | 4.02 | 4.19 | 3.76 | **0.05** | (+)* | 3.95 | 4.08 | 0.83 | (-) | 4.43 | 3.91 | **0.03** | (+)* |
| Já atuei como defensor(a) da privacidade ("privacy champion") em minha equipe ou empresa. | S19 | 2.77 | 2.81 | 2.71 | 0.35 | (+) | 2.82 | 2.76 | 0.40 | (+) | 3.57 | 2.54 | **0.00** | (+)** |
| Ao lidar com conflitos de privacidade com clientes, procuro negociar para implementar controles de privacidade. | S20 | 3.43 | 3.43 | 3.44 | 0.50 | (+) | 3.39 | 3.48 | 0.57 | (-) | 4.00 | 3.25 | **0.01** | (+)** |
| Já enfrentei solicitações suspeitas de clientes para coleta excessiva de dados. | S21 | 2.76 | 2.57 | 3.06 | 0.94 | (-)* | 3.05 | 2.20 | **0.01** | (+)** | 3.79 | 2.48 | **0.00** | (+)*** |

Fonte: Elaborada pela autora (2025).

**Níveis de magnitude (d):** Insignificante (sem símbolo), pequena (*), média (**) e grande (***). As magnitudes positivas são representadas pelo símbolo (+) e as negativas pelo símbolo (-).

sobre leis de privacidade **[S1]**, iniciativa para aprendizado **[S4]** e abordagem de questões de privacidade **[S16]**. Participantes com experiência direta em privacidade relataram consciência ligeiramente maior das leis e padrões de privacidade relevantes, com uma diferença quase significativa ($p$=0,07). Os participantes com experiência direta demonstraram maior iniciativa em aprender sobre privacidade de forma independente, tendência

apoiada por um resultado marginalmente significativo ($p$=0,08). Identificar problemas de privacidade durante o desenvolvimento foi mais comum entre participantes com funções diretas em privacidade, evidenciado pela diferença significativa ($p$=0,10). Esses achados sugerem que o envolvimento direto em trabalhos relacionados à privacidade impacta positivamente a conscientização auto-relatada e comportamentos proativos de aprendizado.

**Organizações Grandes vs. Pequenas.** Participantes de organizações maiores tiveram probabilidade significativamente maior de participar de treinamentos em privacidade ($p$=0,01) **[ S3]**, indicando oportunidades estruturadas em locais de trabalho maiores. Além disso, eles obtiveram pontuações mais altas na compreensão de leis relevantes, como ISO/IEC 29100 e Privacy by Design **[ S1]**, com diferença estatisticamente significativa ($p$=0,02). Adicionalmente, frequentemente aplicam esse conhecimento em atividades diárias ($p$=0,04) **[ S2]**. Essa tendência reflete maior ênfase em educação formal e recursos sobre privacidade em empresas maiores comparadas às menores.

**Funções de Especialista vs. Não-Especialista.** Especialistas relataram consistentemente maior conhecimento sobre leis de privacidade e sua aplicação ($p$<0,00 para **[ S1]**, $p$=0,04 para **[ S2]**). Além disso, esse conhecimento é obtido por iniciativa própria, incluindo leitura de leis e regulamentos de privacidade e consulta a especialistas ($p$<0,00 para **[ S4]**). Eles também demonstraram maior consciência de riscos, como acesso não autorizado e vazamento de dados **[S5]**, embora essa diferença não tenha sido estatisticamente significativa ($p$=0,12). No entanto, foi observada diferença estatisticamente significativa ($p$<0,00) quanto à consciência das melhores práticas e técnicas para proteger a privacidade do usuário em sistemas de *software*, incluindo anonimização de dados e práticas de controle de acesso **[ S6]**. Observação semelhante aplica-se à **[ S7]** com $p$=0,04, sobre o conhecimento de que a privacidade vai além da proteção de dados e inclui aspectos como controle sobre os dados e consentimento informado.

Além disso, os especialistas têm mais probabilidade de se preocupar com a possibilidade de serem monitorados ou manipulados ao usar aplicativos, redes sociais ou navegar na internet ($p$<0,02 para **[ S8]**). Adicionalmente, eles eram muito mais propensos a identificar problemas de privacidade durante atividades de desenvolvimento ($p$<0,00 para **[ S16]**), a propor soluções para problemas de privacidade encontrados durante o desenvolvimento de *software* ($p$=0,03 para **[ S18]**) e a atuar como "campeões da privacidade" em suas organizações ($p$<0,00 para **[ S19]**). De forma similar, os especialistas foram mais ativos na negociação de conflitos relacionados à privacidade com clientes ($p$=0,01 para **[ S20]**) e já enfrentaram solicitações suspeitas de coleta excessiva de dados por parte de clientes ($p$<0,00 para **[ S21]**). Esses resultados enfatizam o papel crucial dos especialistas na promoção da conscientização sobre privacidade e na incorporação de práticas de privacidade nos processos de desenvolvimento.

**Comparações entre grupos.** Foi possível observar diferenças significativas quando múltiplos fatores foram examinados juntos: (1) Participantes com experiência direta e aqueles especializados em privacidade eram mais propensos a propor soluções para problemas de privacidade ($p$=0,05 e $p$=0,03 para **[ S18]**); (2) De forma semelhante, os grupos que trabalham em grandes organizações e os especialistas já enfrentaram solicitações suspeitas de coleta excessiva de dados por parte de clientes ($p$=0,01 e $p$<0,00 para **[ S21]**). Essas observações mostram os efeitos da sinergia da experiência, especialização e tamanho da organização na melhoria das práticas de privacidade.

De forma geral, os participantes demonstraram um nível moderado a alto de concordância com afirmações relacionadas à conscientização sobre privacidade de dados, sugerindo que a consciência sobre conceitos relacionados à privacidade é ampla, mas varia significativamente entre certos grupos e contextos. Portanto, tais achados destacam a necessidade de estratégias personalizadas para melhorar a conscientização e a integração de práticas de privacidade em diferentes contextos de desenvolvimento de *software*. Complementarmente, foi solicitado aos participantes que descrevessem

as razões para sua classificação em relação às afirmações com as quais discordaram fortemente (Q19). A maioria dos participantes que respondeu a essa pergunta indicou que isso se devia à falta de conhecimento sobre leis de privacidade ou à falta de treinamento.

> *#P16 disse: "Não li nenhuma regulamentação específica sobre privacidade, nem recebi qualquer treinamento sobre isso em minha organização. Há pessoas na equipe com mais experiência que lidam com essa atividade[...]"*

Para as afirmações com as quais o participante discordou fortemente em (Q20), foi solicitado que descrevessem os motivos de sua classificação (Q21). Os participantes que responderam a essa pergunta expressaram discordância, citando a falta de padronização na definição do que constitui privacidade, a conscientização insuficiente sobre práticas de privacidade dentro das organizações e a ausência de equipes especializadas focadas em privacidade e proteção de dados nas organizações.

> *#P101 disse: "Acredito que as equipes de desenvolvimento de software já estão sobrecarregadas com outras tarefas técnicas e gerenciais. É necessário que as organizações tenham uma equipe dedicada à privacidade de dados e ao tratamento de dados pessoais para supervisionar e apoiar a equipe de desenvolvimento durante suas atividades."*

Os participantes discordaram fortemente (Q23) porque acreditam que ainda há falta de conscientização das pessoas sobre a importância da privacidade de dados.

> *#P116 disse: "Ainda é muito difícil convencer as pessoas sobre a importância da privacidade. Embora a resistência fosse maior no passado, ela ainda persiste. Acredito que as pessoas ainda estão começando a compreender os benefícios da privacidade."*

**Achado 2:** A conscientização sobre privacidade de dados é complexa, com variações influenciadas pela experiência direta em privacidade, pelo tamanho da organização e pela especialização profissional. Essas diferenças ressaltam a importância de intervenções direcionadas, como treinamento em privacidade em organizações menores e o incentivo a que profissionais não especializados se envolvam com conceitos de privacidade.

## 5.3 Percepção dos Desenvolvedores sobre Estratégias de Privacidade de Dados (QP2)

A $\mathbf{QP}_2$ foi abordada por meio da análise da percepção dos desenvolvedores sobre 13 estratégias de privacidade de dados com base em três fatores: frequência de uso (Q25), importância percebida (Q27) e facilidade de uso (Q29). Adicionalmente, foram examinadas as respostas de Q24 sobre a frequência de utilização das estratégias de privacidade de dados nas fases de desenvolvimento, bem como os *insights* das perguntas abertas em Q26 e Q28. Os procedimentos de análise empregados para responder à $QP_2$ são detalhados na Seção 4.2.6.2.

**Frequência de uso das estratégias de privacidade de dados nas fases de desenvolvimento.** A Tabela 2 apresenta uma visão geral das respostas de Q24, sobre com que frequência os desenvolvedores aplicam estratégias de privacidade de dados nas diferentes fases de desenvolvimento de *software*.

Observa-se que as fases de *Codificação* e *Manutenção* apresentam uma adoção relativamente maior das estratégias de privacidade de dados, com contagens significativas de respostas Sempre e Frequentemente (38 e 25 Sempre, respectivamente, e 21 e 29 Frequentemente). Além disso, a fase de *Análise de Requisitos* demonstra uma combinação de uso frequente (Sempre = 19, Frequentemente = 38) e uso ocasional (Às Vezes = 19), sugerindo que se trata de uma fase crítica, mas abordada de forma variável.

Tabela 2 – Frequência das estratégias de privacidade nas fases de desenvolvimento

| Fase de Desenvolvimento | Frequência | | | | | |
|---|---|---|---|---|---|---|
| | **Nunca** | **Raramente** | **Às vezes** | **Frequentemente** | **Sempre** | **Total** |
| **Análise de requisitos** | 3 (3,41%) | 9 (10,23%) | 19 (21,59%) | 38 (43,18%) | 19 (21,59%) | 88 |
| ***Design*** | 11 (12,5%) | 15 (17,05%) | 27 (30,68%) | 20 (22,73%) | 15 (17,05%) | 88 |
| **Codificação** | 4 (4,55%) | 8 (9,09%) | 17 (19,32%) | 21 (23,86%) | 38 (43,18%) | 88 |
| **Estudo de viabilidade** | 10 (11,36%) | 14 (15,91%) | 23 (26,14%) | 23 (26,14%) | 18 (20,45%) | 88 |
| **Instalação** | 15 (17,05%) | 14 (15,91%) | 27 (30,68%) | 17 (19,32%) | 15 (17,05%) | 88 |
| **Implantação** | 14 (15,91%) | 15 (17,05%) | 19 (21,59%) | 24 (27,27%) | 16 (18,18%) | 88 |
| **Testes** | 8 (9,09%) | 8 (9,09%) | 24 (27,27%) | 21 (23,86%) | 27 (30,68%) | 88 |
| **Manutenção** | 5 (5,68%) | 7 (7,95%) | 22 (25%) | 29 (32,95%) | 25 (28,41%) | 88 |

Fonte: Elaborada pela autora (2025).

Fases como *Design* e *Implantação* apresentam relativamente menos respostas Sempre (15 e 16, respectivamente) e um uso mais moderado (Às Vezes e Raramente). Isso indica uma possível lacuna na integração de estratégias de privacidade durante essas fases. Por fim, as fases de *Estudo de Viabilidade* e *Instalação* têm menos desenvolvedores aplicando estratégias de privacidade de forma consistente (Sempre = 18 e 15), e um número notável de respostas Nunca (10 e 15), indicando priorização limitada nessas áreas.

**Achado 3:** As estratégias de privacidade de dados são consistentemente utilizadas nas fases de *Codificação*, *Testes* e *Manutenção*. Em contraste, as fases de *Design* e *Estudo de Viabilidade* mostraram uma adoção menos consistente, destacando áreas que precisam de melhorias na integração de práticas de privacidade ao longo de todo o ciclo de desenvolvimento.

**Análise da frequência de uso, importância percebida e facilidade de uso das estratégias de privacidade de dados.** A Tabela 3 apresenta uma análise comparativa de várias estratégias de privacidade de dados com base em três métricas: frequência de uso, importância percebida e facilidade de uso. Os dados são apresentados em formato de mapa de calor, em que a intensidade das cores reflete a magnitude dos valores correspondentes de cada métrica para cada estratégia. Nesse contexto, a cor mais verde destaca estratégias amplamente utilizadas, altamente importantes e consideradas fáceis

de usar. Por outro lado, a cor vermelha indica estratégias menos frequentemente adotadas, percebidas como menos importantes ou mais difíceis de usar. Em outras palavras, quanto mais verde uma estratégia aparecer, mais ela é reconhecida por sua utilidade, importância ou praticidade. Por outro lado, tons mais vermelhos sugerem menor priorização ou adoção na prática.

Tabela 3 – Comparação da frequência de uso, importância percebida e facilidade de uso das estratégias de privacidade de dados

| Estratégia de Privacidade de Dados | Frequência de Uso | Importância Percebida | Facilidade de Uso |
|---|---|---|---|
| Criptografia | 76,46% | 94,02% | 68,51% |
| Minimização da coleta de dados pessoais | 71,40% | 85,76% | 71,82% |
| Descentralização | 58,58% | 75,08% | 57,07% |
| Soberania de dados | 67,79% | 82,21% | 60,68% |
| Dados temporais | 64,53% | 78,10% | 65,66% |
| Controle do usuário | 77,20% | 86,89% | 69,41% |
| Desativar coleta de dados | 56,20% | 73,65% | 72,68% |
| Anonimização | 69,07% | 84,74% | 62,04% |
| Ferramentas de classificação de dados | 60,45% | 77,13% | 61,38% |
| Revisão de design e código | 72,62% | 83,78% | 66,44% |
| Gerenciamento de riscos | 70,28% | 89,86% | 61,15% |
| Modelagem de fluxo de dados | 69,12% | 83,25% | 63,48% |
| Proxy | 57,61% | 72,22% | 59,76% |

Fonte: Elaborada pela autora (2025).

Ao analisar os padrões de cores, é possível observar que as três estratégias mais frequentemente utilizadas foram: *Controle do usuário* (77,20%), *Criptografia* (76,46%) e *Revisão de design e código* (72,20%). Quanto às estratégias de privacidade com maior importância percebida, observa-se que a maioria das estratégias é considerada importante, sendo que as estratégias de *Criptografia* (94,02%), *Gestão de riscos* (89,86%) e *Controle do usuário* (86,89%) aparecem no top 3. Por outro lado, a maioria das estratégias é percebida como não fácil de usar, exceto *Desativar coleta de dados* (72,68%) e *Minimização da coleta de dados pessoais* (71,82%), que apresentam valores moderados. Além disso, também é possível observar que *Desativar coleta de dados* possui a menor frequência de uso (56,20%), apesar de sua facilidade de uso e importância moderada. Em resumo, esta análise ajuda a priorizar estratégias com base em sua frequência de uso, importância percebida e facilidade de uso.

**Achado 4:** Embora certas estratégias, como *Criptografia*, sejam amplamente utilizadas e percebidas como altamente importantes, outras, como *Desativar coleta de dados*, destacam estratégias em que a facilidade de uso não necessariamente leva à adoção generalizada.

**Análise da correlação entre frequência de uso, importância percebida e facilidade de uso.** Com o objetivo de compreender de forma mais aprofundada a relação entre as estratégias de privacidade de dados, foi realizada uma análise de correlação entre a frequência de uso, importância percebida e facilidade de uso relatadas pelos participantes (N = 88). Desse modo, formulou-se hipótese alternativa **HA**1**:** Há uma forte correlação entre a frequência de uso e a importância percebida na [*estratégia de privacidade*]$n$. A hipótese nula é **HA**0**:** Não há forte correlação entre frequência de uso e importância percebida na [*estratégia de privacidade*]$n$.

Adicionalmente, foi formulado a hipótese alternativa **HB**1**:** Há uma forte correlação entre a importância percebida e a facilidade de uso na [*estratégia de privacidade*]$n$. A hipótese nula é **HB**0**:** Não há forte correlação entre importância percebida e facilidade de uso na [*estratégia de privacidade*]$n$. De forma similar, foi hipotetizado que **HC**1**:** Há uma forte correlação entre facilidade de uso e frequência de uso na [*estratégia de privacidade*]$n$. A hipótese nula é **HC**0**:** Não há forte correlação entre facilidade de uso e frequência de uso na [*estratégia de privacidade*]$n$.

Foi aplicado o teste de *Shapiro-Wilk* (SHAPIRO; WILK, 1965) para avaliar a distribuição de nossos dados. Confirmamos que os dados não seguem uma distribuição normal. Diante desse resultado, optou-se pelo uso do *Spearman's rank correlation coefficient* (WOHLIN *et al.*, 2012). Foi considerado o intervalo de confiança de 95% ($p$-valor $< 0,05$). Como resultado, foi obtido um $p$-valor $< 0,01$ para todas as estratégias de privacidade de dados em todas as correlações. Portanto, as correlações calculadas apresentam significância estatística para todas as estratégias de privacidade de dados.

A Tabela 4 apresenta os resultados da correlação. A primeira coluna lista cada estratégia de privacidade de dados. A segunda coluna apresenta a correlação entre a importância percebida e a frequência de uso. A terceira coluna apresenta a correlação entre a importância percebida e a facilidade de uso. Por fim, a última coluna apresenta a correlação entre a facilidade de uso e a frequência de uso.

Os valores de correlação foram classificados de acordo com um trabalho anterior (SALKIND, 2012): Relação muito forte (0,8 a 1,0 ou -0,8 a -1,0); Relação forte (0,6 a 0,8 ou -0,6 a -0,8); Relação moderada (0,4 a 0,6 ou -0,4 a -0,6); Relação fraca (0,2 a 0,4 ou -0,2 a -0,4); e Relação fraca ou inexistente (0,0 a 0,2 ou 0,0 a -0,2).

Tabela 4 – Correlação de *Spearman* entre frequência de uso, importância percebida e facilidade de uso das estratégias de privacidade de dados

| **Estratégia de Privacidade de Dados** | **Correlação (Importância, Uso)** | | **Correlação (Importância, Facilidade)** | | **Correlação (Facilidade, Uso)** | |
|---|---|---|---|---|---|---|
| | **Estatística (rho)** | **Categoria** | **Estatística (rho)** | **Categoria** | **Estatística (rho)** | **Categoria** |
| Criptografia | 0,770 | Forte | 0,676 | Forte | 0,536 | Moderada |
| Minimização da coleta de dados pessoais | 0,719 | Forte | 0,691 | Forte | 0,557 | Moderada |
| Descentralização | 0,661 | Forte | 0,633 | Forte | 0,662 | Forte |
| Soberania de dados | 0,736 | Forte | 0,621 | Forte | 0,567 | Moderada |
| Dados temporais | 0,643 | Forte | 0,514 | Moderada | 0,438 | Moderada |
| Controle do usuário | 0,785 | Forte | 0,696 | Forte | 0,601 | Forte |
| Desativar coleta de dados | 0,550 | Moderada | 0,525 | Moderada | 0,388 | Fraca |
| Anonimização | 0,658 | Forte | 0,506 | Moderada | 0,530 | Moderada |
| Ferramentas de classificação de dados | 0,635 | Forte | 0,574 | Moderada | 0,443 | Moderada |
| Revisão de design e código | 0,647 | Forte | 0,609 | Forte | 0,533 | Moderada |
| Gerenciamento de riscos | 0,756 | Forte | 0,568 | Moderada | 0,427 | Moderada |
| Modelagem de fluxo de dados | 0,673 | Forte | 0,510 | Moderada | 0,465 | Moderada |
| Proxy | 0,647 | Forte | 0,594 | Moderada | 0,421 | Moderada |

Fonte: Elaborada pela autora (2025).

Ao analisar a Tabela 4, é possível observar que há uma alta correlação entre **importância percebida e frequência de uso** nas estratégias de privacidade de dados. Mais especificamente, estratégias de privacidade como *Controle do usuário* ($\rho$=0,785), *Criptografia* ($\rho$=0,770) e *Gestão de riscos* ($\rho$=0,756) apresentam fortes correlações, indicando que os usuários tendem a adotar essas estratégias com frequência quando as percebem como altamente importantes. No entanto, a estratégia *Desativar coleta de dados* ($\rho$=0,55) mostra uma correlação moderada, sugerindo que sua importância percebida pode nem sempre estar correlacionada à frequência de uso. Portanto, tais resultados confirmam $HA_1$ para todas as estratégias de privacidade de dados, exceto

para a estratégia *Desativar coleta de dados*. Para essa estratégia, rejeitamos $HA_1$ (e confirmamos $HA_0$).

A correlação entre **importância percebida e facilidade de uso** mostrou que estratégias como *Controle do usuário* ($\rho$=0,696), *Minimização da coleta de dados pessoais* ($\rho$=0,691) e *Criptografia* ($\rho$=0,676) apresentam fortes correlações, indicando que a facilidade de uso influencia significativamente como os usuários percebem a importância dessas estratégias. Por outro lado, estratégias como *Dados temporais* ($\rho$=0,514) e *Anonimização* ($\rho$=0,506) apresentam correlações moderadas, sugerindo que desafios de usabilidade podem reduzir a importância percebida. Assim, a $HB_1$ foi confirmada para as seguintes estratégias: *Controle do usuário*, *Soberania de dados*, *Descentralização*, *Minimização da coleta de dados pessoais*, *Revisão de design e código* e *Criptografia*. Para as demais estratégias, rejeitamos $HB_1$ (e confirmamos $HB_0$).

Em relação à correlação entre **facilidade de uso e frequência de uso**, a maioria das estratégias apresenta correlações moderadas nesta categoria, como *Proxy* ($\rho$=0,421), *Gestão de riscos* ($\rho$=0,427) e *Modelagem de fluxo de dados* ($\rho$=0,465), indicando que a usabilidade influencia parcialmente a adoção, mas pode não ser o único fator. Por outro lado, as estratégias *Descentralização* ($\rho$=0,662) e *Controle do usuário* ($\rho$=0,601) foram as únicas a demonstrarem forte correlação, indicando que a facilidade de uso tem impacto positivo na adoção dessas estratégias. Além disso, a estratégia *Desativar coleta de dados* ($\rho$=0,388) foi a única a apresentar correlação fraca, sugerindo que a facilidade de uso tem impacto limitado na frequência de adoção. Assim, foi confirmada $HC_1$ apenas para as estratégias *Descentralização* e *Controle do usuário*. Para as demais estratégias, rejeitamos $HC_1$ (e confirmamos $HC_0$).

**Achado 5:** A maioria das estratégias de privacidade de dados, 92% (12/13), apresentou forte correlação entre importância percebida e frequência de uso. Além disso, 38% (5/13) mostraram forte correlação entre importância percebida e facilidade de uso, enquanto 61% (8/13) apresentaram correlação moderada. Por fim, facilidade de uso e frequência de uso apresentaram correlação moderada em 84% (11/13) das estratégias, com uma estratégia apresentando correlação fraca.

**Estratégias de privacidade de dados específicas nas correlações.** Na análise dos padrões associados a estratégias específicas, verificou-se que *Criptografia*, *Minimização da coleta de dados pessoais*, *Soberania de dados* e *Controle do usuário* apresentaram alta correlação em todas as três dimensões (Forte tanto em Importância–Uso quanto em Importância–Facilidade; e Moderada em Facilidade–Uso). Isso sugere que essas estratégias de privacidade são valorizadas e frequentemente utilizadas, apesar de desafios moderados de usabilidade. Por outro lado, *Descentralização* foi a única estratégia que demonstrou forte correlação em todas as dimensões, sugerindo um alinhamento consistente entre importância percebida, facilidade de uso e frequência de uso. Além disso, *Desativar coleta de dados* foi a única estratégia que apresentou as correlações mais fracas em todas as dimensões, particularmente em Facilidade–Uso ($\rho$=0,367). Isso pode refletir barreiras de usabilidade ou relevância percebida limitada em contextos específicos. Em contrapartida, a estratégia *Controle do usuário* apresenta as maiores correlações em Importância–Uso ($\rho$=0,777), enfatizando a necessidade de ferramentas que capacitem os usuários a gerenciar seus dados.

Também foi questionado aos participantes se eles utilizam estratégias adicionais de implementação para garantir a privacidade de dados (Q26) que não foram mencionadas na pergunta anterior (Q25) e, em caso afirmativo, quais são essas estratégias. Apenas sete participantes responderam a essa pergunta e mencionaram o uso de ferramentas como *Static Application Security Testing (SAST)*, *Dynamic Application*

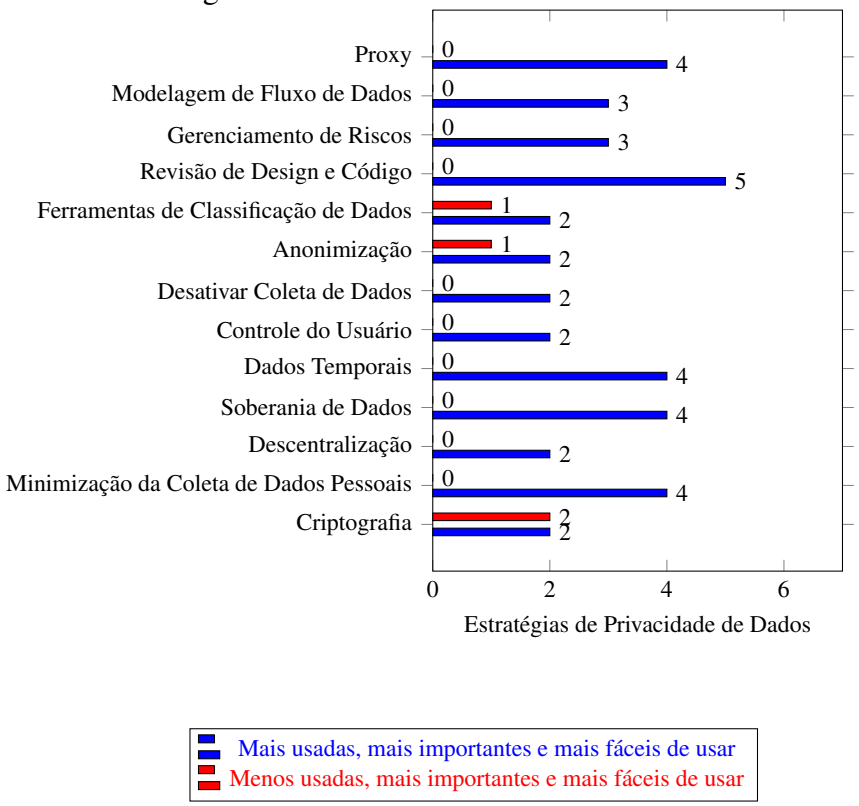
*Security Testing (DAST)*, *Data Loss Prevention (DLP)* e *Virtual Private Network (VPN)*.

> **Achado 6:** Estratégias de privacidade como *Criptografia*, *Descentralização* e *Controle do usuário* surgem como eficazes e amplamente adotadas, refletindo seu forte alinhamento entre importância percebida, usabilidade e frequência de uso. Em contraste, estratégias como *Desativar coleta de dados* e *Dados temporais* destacam a necessidade de melhorias direcionadas para aumentar sua usabilidade e relevância percebida, incentivando uma adoção mais ampla.

**Análise das interseções entre frequência de uso, importância percebida e facilidade de uso.** Foi realizada uma análise da ocorrência de cada estratégia de privacidade em quatro categorias: (1) *Mais usada, mais importante e mais fácil de usar*; (2) *Menos usada, menos importante e mais difícil de usar*; (3) *Mais usada, menos importante e mais difícil de usar*; e (4) *Menos usada, mais importante e mais fácil de usar*. Esta análise foi baseada na escala Likert, em que 5 indica *mais*, *mais importante* e *mais fácil*, enquanto 1 indica *menos* e *mais difícil*. A Figura 10 mostra a frequência das estratégias de privacidade dentro dessas quatro categorias.

Ao analisar a Figura 10, foi possível observar que cada estratégia de privacidade de dados aparece pelo menos uma vez na categoria (1): *Mais usada, mais importante e mais fácil de usar*. Mais especificamente, a estratégia *Revisão de Design e Código* aparece cinco vezes, seguida pelas estratégias *Dados Temporais*, *Soberania de Dados*, *Proxy* e *Minimização da Coleta de Dados Pessoais*, cada uma com quatro ocorrências, respectivamente. Além disso, observa-se, ainda, que na categoria (4): *Menos usada, mais importante e mais fácil de usar*, a estratégia *Criptografia* aparece duas vezes, seguida por *Anonimização* e *Ferramentas de Classificação de Dados*, com uma ocorrência cada, respectivamente. Por fim, nenhuma estratégia de privacidade de dados aparece simultaneamente na categoria *Menos usada, menos importante e mais difícil de usar*. Essa observação também se aplica à terceira categoria, ou seja, *Mais usada, menos*

Figura 10 – Distribuição das estratégias de privacidade de dados nas categorias




Fonte: Elaborada pela autora (2025).

*importante e mais difícil de usar*.

Em relação às estratégias que os participantes consideraram importantes, pedimos que explicassem os motivos de suas avaliações (Q28). Os respondentes afirmaram que todas as estratégias apresentadas na pesquisa são importantes.

> *#P30 disse: "Todas as opções fornecem um nível adicional de privacidade para os dados do usuário. O uso de cada estratégia depende do cenário em que será aplicada. Por exemplo, a criptografia pode ser usada para senhas de usuários, enquanto o controle de dados está mais relacionado tanto a permissões quanto à privacidade do sistema, garantindo que os usuários evitem acessos não autorizados. A revisão de código é essencial*

*para garantir que nada que possa afetar a privacidade dos dados seja introduzido na produção do sistema."*

**Achado 7:** Nenhuma estratégia de privacidade de dados é simultaneamente classificada como *Menos usada, menos importante e mais difícil de usar*. De forma similar, nenhuma aparece na categoria *Mais usada, menos importante e mais difícil de usar*. Por outro lado, todas as estratégias de privacidade de dados aparecem pelo menos duas vezes na categoria *Mais usada, mais importante e mais fácil de usar*.

## 5.4 Aderência às Práticas de Privacidade de Dados em Organizações de *Software* (QP3)

Para responder à $QP_3$, foi conduzida uma análise dos fatores organizacionais que influenciam a adoção de práticas de privacidade de dados, com base nas respostas às questões Q30, Q32 e Q33. Adicionalmente, foram analisadas as respostas de duas perguntas abertas: (i) Q31, que explora a dinâmica de trabalho e práticas organizacionais para lidar com privacidade e proteção de dados, e (ii) Q34, que captura as percepções de desenvolvedores brasileiros sobre desafios organizacionais na proteção dos direitos de privacidade dos usuários. Os procedimentos de análise são detalhados na Seção 4.2.6.3.

**Influência de fatores organizacionais na adoção de estratégias de privacidade.** Com o objetivo de compreender como fatores organizacionais influenciam a adoção de estratégias de privacidade pelas equipes de desenvolvimento, foram examinados três aspectos principais: (ver Tabela 5): *(i)* a presença de equipes dedicadas à privacidade (Q30), *(ii)* o uso de ferramentas específicas para gerenciamento de dados privados (Q32), e *(iii)* a prioridade percebida dada pelas organizações à privacidade e proteção de dados (Q33). Nossa análise, baseada em 88 respostas, fornece *insights* sobre estruturas organizacionais e seu impacto nas práticas de privacidade.

Tabela 5 – Estrutura Organizacional e Ferramentas Utilizadas

| **Equipe Dedicada (Q30)** | **#respostas** | **Ferramentas Mais Utilizadas (Q32)** | **Prioridade Organizacional (Q33)** |
|---|---|---|---|
| Sim, equipe interna dedicada | 43 | Nenhuma (58,14%), OneTrust (11,63%), Outras (30,23%) | Essencial (41,86%), Alta (41,86%), Média (16,28%) |
| Não, lidamos de forma ad-hoc | 39 | Nenhuma (89,74%), OneTrust, Ketch, Vanta (2,58%), BigID, Ketch, Vanta (2,56%), Securiti, Vanta (2,56%), OneTrust, Securiti, Ketch (2,56%) | Essencial (17,95%), Média (35,90%), Baixa (20,51%), Alta (15,38%), Não é prioridade (10,26%) |
| Equipe terceirizada | 4 | Nenhuma (75%), OneTrust (25%) | Essencial (50%), Alta (50%) |
| Não sabe / Incerto | 2 | Be Compliance (100%) | Média (100%) |

Fonte: Elaborada pela autora (2025).

*Estruturas organizacionais e gestão de privacidade.* A presença de equipes dedicadas à privacidade emergiu como um fator significativo na adoção de estratégias de privacidade. Entre os participantes pesquisados, 43 relataram ter uma equipe interna exclusivamente focada em privacidade, enquanto 39 lidavam com questões de privacidade de forma ad hoc. Além disso, 4 participantes empregavam equipes de privacidade terceirizadas, enquanto outros mencionaram abordagens híbridas ou não tinham certeza sobre a estrutura de sua organização.

*Adoção de ferramentas e padrões de uso.* Organizações com equipes dedicadas à privacidade eram mais propensas a utilizar ferramentas específicas para gerenciamento de privacidade, sendo o OneTrust o mais frequentemente mencionado (11,63%), seguido por soluções como BigID e sistemas desenvolvidos internamente (cada um com 2,33%). Por outro lado, 89,74% das organizações sem equipes dedicadas relataram não usar nenhuma ferramenta específica de privacidade. Isso demonstra uma correlação clara entre o suporte organizacional estruturado e a adoção de soluções tecnológicas para privacidade. O número de ferramentas empregadas pelas organizações ilustra ainda mais a influência dos fatores estruturais. A maioria dos respondentes (78) relatou usar uma única ferramenta, enquanto um número menor utilizou duas (6 respostas), três (4

respostas) ou até cinco ferramentas (1 resposta).

*Prioridade organizacional percebida.* A prioridade percebida atribuída à privacidade também variou significativamente com base na estrutura organizacional: (i) *Organizações com equipes dedicadas* - Os respondentes predominantemente consideraram a privacidade essencial (41,86%) ou de alta prioridade (41,86%), com apenas 16,28% classificando-a como prioridade média; (ii) *Gestão de privacidade ad hoc* - A percepção de prioridade foi menor, com apenas 17,95% avaliando a privacidade como essencial, enquanto 35,90% a classificaram como prioridade média e 20,51% como baixa; (iii) *Equipes de privacidade terceirizadas* - Metade dos respondentes avaliou a privacidade como essencial, e a outra metade considerou de alta prioridade; e (iv) *Estruturas incertas* - Respondentes que desconheciam a estrutura de gestão de privacidade de sua organização consideraram a privacidade como prioridade média.

**Achado 8:** A ausência de equipes dedicadas à privacidade se correlaciona com menor prioridade percebida e menor investimento em ferramentas, mesmo em organizações que reconhecem a importância da privacidade.

Esses *insights* enfatizam a necessidade de uma abordagem estruturada para a gestão da privacidade, que requer equipes especializadas, ferramentas e compromisso organizacional para priorizar a privacidade no desenvolvimento de *software*. Abordar essas lacunas melhorará as estratégias de privacidade e protegerá de forma mais eficaz os dados dos usuários no cenário digital em constante evolução.

De fato, a partir do achado 8, a cultura organizacional desempenha um papel crucial na forma como decisões sobre privacidade são tomadas. Vários participantes mencionaram que sua capacidade de implementar medidas de privacidade foi influenciada, seja apoiada ou limitada, pelas prioridades da gestão, pelos recursos disponíveis e pela postura geral da organização em relação à privacidade. Na prática, isso significa que os desenvolvedores podem ser tanto empoderados quanto limitados por decisões

tomadas em níveis hierárquicos superiores. Por exemplo, se a privacidade não for tratada como prioridade pela liderança, torna-se muito mais difícil para os desenvolvedores justificar o tempo e esforço necessários para implementar proteções robustas. Por outro lado, quando a privacidade é apoiada de cima para baixo, com políticas claras, treinamento e recursos dedicados, os desenvolvedores estão melhor posicionados para tomar decisões informadas e integrar a privacidade de forma eficaz em seu trabalho. Embora nosso estudo não tenha focado especificamente na cultura organizacional, esses aspectos emergiram nas respostas qualitativas, sugerindo que os desenvolvedores frequentemente são limitados por decisões tomadas em níveis superiores.

**A dinâmica de trabalho e práticas organizacionais para lidar com privacidade e proteção de dados.** Para compreender melhor como as organizações abordam questões de privacidade de dados, foi solicitado aos participantes que descrevessem as dinâmicas de trabalho e práticas específicas que suas organizações utilizam para gerenciar privacidade e proteção de dados (Q31 do Apêndice B). Um total de 88 participantes respondeu a essa questão, a partir da qual foram identificadas nove categorias (ver Quadro 4).

Os achados deste estudo são semelhantes aos do estudo realizado por Canedo *et al.* (2021), que conduziu uma pesquisa com 82 profissionais de empresas de desenvolvimento de *software* de diversas organizações, bem como um grupo focal com 11 participantes, para entender como os princípios da LGPD são implementados pelas equipes de desenvolvimento de *software*. A maioria dos participantes afirmou que a privacidade de dados deve ser aplicada pelas equipes de desenvolvimento utilizando técnicas como criptografia e anonimização de dados.

Franke *et al.* (2024) conduziu um estudo com 56 desenvolvedores de *software* open-source (OSS) para compreender o impacto da implementação do Regulamento Geral de Proteção de Dados (GDPR) nas atividades de desenvolvimento. A maioria dos participantes reconheceu que a implementação dos conceitos do GDPR afeta os

Quadro 4 – Dinâmica de trabalho para lidar com privacidade e proteção de dados

| Categoria | Subcategoria | # |
|---|---|---|
| 1. Leis | Análise dos dados coletados | 14 |
| | Legislação, consentimento, gerenciamento de riscos e anonimização | 1 |
| | Sistema de governança de dados sob regras e diretrizes | 1 |
| | Falta de experiência prática em privacidade | 1 |
| | Análise de conformidade com a LGPD no processo de desenvolvimento | 1 |
| | Minimização de dados e proteção da identidade do usuário | 1 |
| | Uso de um banco de dados unificado | 1 |
| | Limitação de acesso a dados | 1 |
| | Aplicação das diretrizes da LGPD e criptografia | 1 |
| | Aplicação do Privacy by Design | 1 |
| | Uso de políticas de privacidade | 1 |
| 2. Equipe de Conformidade | Existe uma equipe de conformidade | 15 |
| 3. Equipe de Desenvolvimento | Discussão e decisão coletiva | 5 |
| | Aplicação da LGPD desde a fase de elicitação de requisitos | 4 |
| | Integração da privacidade no processo de definição de requisitos | 1 |
| | Responsabilidade do desenvolvedor pelo ciclo de vida dos dados | 1 |
| | Durante o desenvolvimento de *software* | 1 |
| | Orientação de membros seniores | 1 |
| | Revisão por pares | 1 |
| 6. Técnicas | Uso de técnicas de anonimização | 2 |
| | Implementação de requisitos de segurança | 1 |
| | Gestão de dados sensíveis e anonimização | 1 |
| | Testes de phishing | 1 |
| | Técnicas de prevenção | 1 |
| | Uso de criptografia | 1 |
| | Controle de acesso, perfis de usuário e gestão de dados | 1 |
| 5. Treinamento | Treinamento e conscientização | 2 |
| | Conscientização de clientes | 1 |
| | Realização de seminários e sessões de treinamento | 1 |
| | Realização de cursos | 1 |
| | Programas de conscientização | 1 |
| 6. Dinâmica de Trabalho | Falta de dinâmica de trabalho | 1 |
| 7. Técnicas e Treinamento | Criptografia; Falta de treinamento | 1 |
| 8. Equipe de Conformidade e Treinamento | Existe uma equipe de conformidade; Falta de treinamento | 1 |
| 9. Legislação; Treinamento; Conscientização; e Técnicas | Governança e Políticas de Privacidade; Treinamento e Conscientização de Funcionários; Controles de Acesso e Segurança Tecnológica; Auditoria e Monitoramento Contínuo; Gestão de Incidentes e Resposta Rápida; Avaliação de Impacto Preventiva | 1 |

Fonte: Elaborado pela autora (2025).

processos de desenvolvimento, destacando a influência dos requisitos de privacidade e conformidade no desenvolvimento de *software* open-source. Quinze desenvolvedores OSS relataram consultar equipes jurídicas para garantir conformidade com o GDPR, e sete participantes com experiência em consulta a equipes de conformidade observaram um impacto positivo em suas atividades de desenvolvimento de *software*.

Os participantes enfatizaram os benefícios de buscar *expertise* jurídica, afirmando a importância de consultar equipes de conformidade para esclarecer requisitos de privacidade e evitar interpretações equivocadas da legislação. Essa consulta facilitou a implementação da conformidade com o GDPR. Os achados deste estudo também reforçam os de Franke *et al.* (2024), pois a maioria dos participantes em nosso estudo relatou que suas dinâmicas e práticas de trabalho para gerenciar privacidade e proteção de dados em suas organizações incluem a consulta a equipes de conformidade.

**Achado 9:** As práticas-chave para gerenciar privacidade e proteção de dados incluem a adesão às leis, como a LGPD, o envolvimento das equipes de conformidade e desenvolvimento e a implementação de técnicas como anonimização e medidas de segurança. Além disso, programas de treinamento são essenciais para aumentar a conscientização dos funcionários e promover uma gestão eficaz da privacidade.

Esses achados reforçam a importância de integrar expertise legal e consulta de conformidade no desenvolvimento de *software* para abordar os desafios de privacidade de forma eficaz.

**Desafios organizacionais na proteção dos direitos de privacidade dos usuários.** Também foi investigado a percepção dos participantes sobre os maiores desafios que as organizações enfrentarão nos próximos anos em relação a práticas e regulamentações para proteger melhor os direitos de privacidade dos usuários (Q34 do Apêndice B). Um total de 87 participantes respondeu a essa questão, e oito categorias

foram identificadas. As categorias mais frequentemente mencionadas foram `Leis de Privacidade` e `IA Generativa`. Cinquenta e três participantes afirmaram que o maior desafio será a implementação das leis de privacidade, enquanto 16 mencionaram lidar com IAs generativas. O Quadro 5 apresenta as oito categorias e suas respectivas subcategorias.

Quadro 5 – Desafios futuros para organizações na proteção dos direitos de privacidade dos usuários

| **Categoria** | **Subcategoria** | **#** |
|---|---|---|
| 1. Leis de privacidade | Implementação de políticas de privacidade eficazes | 41 |
| | Leis específicas de cada país | 4 |
| | Adaptação de sistemas legados | 2 |
| | Implementação de auditoria e coleta de dados seguras | 1 |
| | Falta de conhecimento | 1 |
| | Falta de ferramentas para apoiar a implementação | 1 |
| | Cibersegurança e transparência | 1 |
| | Segurança | 1 |
| | Falta de ferramentas para otimizar processos | 1 |
| 2. IA generativa | Lidar com IAs generativas | 15 |
| | Viés nos dados de treinamento | 1 |
| 3. Leis de privacidade; IA generativa | Implementação de políticas de privacidade eficazes; Lidar com IAs generativas | 4 |
| 4. Leis de privacidade; IA generativa; Conscientização | Implementação de políticas de privacidade eficazes; Lidar com IAs generativas; Falta de conscientização dos usuários | 1 |
| 5. Conscientização | Falta de conscientização dos usuários | 2 |
| | Conscientização dos usuários | 1 |
| 6. Engajamento | Engajar pessoas | 3 |
| 7. Treinamento | Falta de equipes especializadas em privacidade | 3 |
| 8. Ciberataques | Ciberataques | 1 |

Fonte: Elaborado pela autora (2025).

Rocha *et al.* (2023) também identificaram, por meio de uma pesquisa com diversos profissionais, que todos os participantes relataram dificuldades na implementação dos princípios da LGPD devido à falta de conhecimento sobre técnicas de implementação. Eles enfatizaram que os profissionais de desenvolvimento de *software* precisam aprimorar sua compreensão das técnicas que garantem privacidade e conformidade com os princípios da LGPD para implementar políticas de privacidade de forma eficaz. Jesus *et al.* (2024) e Peixoto *et al.* (2023) também identificam que os profissionais enfrentam

dificuldades para implementar de maneira eficaz os princípios das leis de privacidade de dados, seja por falta de conhecimento ou pela ausência de ferramentas automatizadas que apoiem a implementação dos requisitos de privacidade durante o processo de desenvolvimento de *software*.

Os achados desse estudo também são semelhantes aos de (GOLDA *et al.*, 2024; CHEUNG; LIU, 2023; FERRARA, 2023), que identificaram desafios relacionados à garantia da privacidade dos dados dos usuários e aos vieses em dados de treinamento ao usar IA generativa.

**Achado 10:** As organizações enfrentam desafios significativos na proteção da privacidade dos usuários, na implementação de políticas eficazes, na adaptação de sistemas legados e no cumprimento de leis diversas. Questões emergentes incluem o gerenciamento de IA generativa e o tratamento de vieses, a conscientização dos usuários, o engajamento das partes interessadas e a formação de equipes especializadas em privacidade.

Com base nesses achados, foi possível observar que enfrentar esses desafios exige uma abordagem multifacetada por parte das organizações. Vários passos concretos podem ajudar a reduzir a lacuna na conscientização sobre privacidade. Um passo-chave é oferecer treinamentos regulares, adaptados a funções específicas e a situações do mundo real, para que os desenvolvedores compreendam de fato como as leis de privacidade se aplicam ao seu trabalho diário. Também é importante incorporar a privacidade nos processos e ferramentas de desenvolvimento, em vez de tratá-la como um aspecto secundário. Além disso, construir uma cultura organizacional onde a privacidade seja levada a sério, começando pela liderança, pode fazer uma grande diferença. Políticas internas claras, colaboração próxima com equipes jurídicas e de *compliance*, e garantir que a privacidade faça parte do planejamento de projetos desde o início ajudam os desenvolvedores a tomar decisões melhores e mais informadas.

Adicionalmente, as organizações brasileiras podem adotar alguns recursos úteis que podem apoiar os desenvolvedores brasileiros a fortalecer seus esforços em privacidade. Por exemplo, adotar os princípios de *Privacy by Design* é um excelente ponto de partida. Existem também padrões bem estabelecidos, como a ISO/IEC 27701, que foca na gestão da informação de privacidade, e orientações práticas da própria Autoridade Nacional de Proteção de Dados (ANPD). Além disso, o *NIST Privacy Framework* pode oferecer passos claros e acionáveis para ajudar as equipes a incorporar a privacidade em seus fluxos de trabalho de desenvolvimento.

## 5.5 Resumo do Capítulo 5

Este capítulo apresentou os principais resultados obtidos a partir dos dados coletados, buscando entender como os desenvolvedores entendem e aplicam questões de privacidade de dados no ciclo de desenvolvimento de *software*. Observou-se que a conscientização sobre privacidade de dados sofre variações conforme a experiência direta com privacidade de dados, conforme o tamanho da organização e conforme a especialização profissional do desenvolvedor. Foi identificado também que estratégias de privacidade são mais utilizadas nas fases de codificação, testes e manutenção. Além disso, foi identificado também que estratégias de privacidade como criptografia, descentralização e controle de usuário são mais eficazes e mais adotadas. Esses achados, reforçam o que foi apontado nos estudos anteriores ao indicar que a privacidade ainda é considerado um requisito secundário e não um princípio inerente ao desenvolvimento de *software*. O próximo capítulo descreve as ameaças à validade do estudo e as estratégias adotadas para sua mitigação.

# 6 AMEAÇAS À VALIDADE DO ESTUDO

Este estudo envolveu uma pesquisa com 88 desenvolvedores, incluindo apenas aqueles participantes que relataram experiência direta ou indireta relacionada à privacidade de dados. Com o intuito de assegurar a validade dos achados, são discutidas a seguir as potenciais ameaças à validade do estudo (WOHLIN *et al.*, 2012) e as estratégias adotadas para sua mitigação.

Primeiramente, em relação *à validade de constructo*, havia o risco de que as questões do questionário não estivessem totalmente alinhadas com os constructos pretendidos, como o entendimento e a experiência dos desenvolvedores em relação à privacidade de dados. Para mitigar isso, as questões do questionário foram elaboradas com base na literatura estabelecida e foram validadas por meio de um estudo piloto com quatro especialistas na área. Esse processo ajudou a garantir que as questões fossem relevantes e capturassem efetivamente os constructos de interesse. As 21 afirmações criadas para responder à QP1 utilizando o modelo *Knowledge-Attitude-Behaviour* (KAB) foram cuidadosamente elaboradas por dois outros pesquisadores envolvidos neste estudo. Além disso, as afirmações foram baseadas em achados de estudos anteriores (IWAYA *et al.*, 2023; TAHAEI *et al.*, 2021; HADAR *et al.*, 2018).

Em segundo lugar, para *a validade interna*, as interpretações das questões pelos participantes poderiam ter sido influenciadas por seus papéis, contextos organizacionais ou experiências prévias, potencialmente introduzindo viés. Para tratar isso, foram fornecidas definições claras e exemplos ilustrativos de termos-chave dentro do instrumento da pesquisa, a fim de minimizar ambiguidades e reduzir a probabilidade de má interpretação. Adicionalmente, foram seguidos procedimentos rigorosos para criar os diferentes grupos utilizados na QP1. Os dados de *background* dos participantes foram coletados e todos os respondentes do questionário foram divididos em diferentes grupos demográficos.

Terceiro, *a validade externa* representou um desafio, uma vez que a generalização dos achados poderia ser limitada devido à natureza auto-selecionada dos participantes e ao foco em indivíduos com experiência em privacidade de dados. Para aumentar a representatividade, buscou-se incluir desenvolvedores de setores e funções profissionais diversos, dentro da indústria de *software* brasileira, garantindo uma ampla variedade de perspectivas sobre práticas de privacidade de dados.

Além disso, foi utilizado uma estratégia de amostragem em bola de neve para ampliar o alcance dos participantes. Embora eficaz para acessar indivíduos com experiência relevante, essa abordagem pode introduzir viés de amostragem, pois os participantes tendem a indicar colegas com *backgrounds* ou perspectivas semelhantes. Para ajudar a mitigar isso, no questionário foram incluídas perguntas de controle relacionadas ao histórico dos participantes (por exemplo, nível de experiência, tamanho da empresa e região), o que permitiu examinar possíveis vieses na amostra. Ainda assim, considera-se que a estratégia de amostragem adotada é apropriada para o contexto brasileiro, onde os registros de desenvolvedores com experiência em privacidade são limitados.

Por fim, em relação *à validade de conclusão*, inconsistências nas respostas dos participantes devido a mal-entendidos ou questões pouco claras poderiam ter impactado a confiabilidade dos achados. Para mitigar essa ameaça, o questionário foi previamente testado e submetido a refinamentos iterativos visando aprimorar a clareza e a consistência do instrumento de pesquisa. Para a análise descritiva e estatística, dois pesquisadores envolvidos neste estudo colaboraram na análise de todas as questões de pesquisa (QPs). Especificamente para a QP1, a distribuição dos dados foi avaliada antes da aplicação dos testes de correlação, a fim de mitigar possíveis vieses na análise estatística. Foram empregados o *Wilcoxon Rank Sum Test* (WHITLEY; BALL, 2002) e o *Cliff's Delta* (d) (GRISSOM; KIM, 2005) para avaliar o nível de concordância com cada afirmação entre os grupos pré-definidos. Adicionalmente, adotou-se o limiar convencional de $p$-valor de 0,05 para estabelecer significância estatística.

O processo de análise de dados descrito na Seção 4.2.6.2 examina as percepções dos participantes sobre a frequência, a importância percebida e a facilidade de uso das estratégias de privacidade de dados, considerando suas características individuais. Essa análise foi baseada em uma pesquisa anterior (DIAS-NETO *et al.*, 2017) e emprega uma abordagem de média ponderada, na qual a ponderação é informada por atributos qualitativos de cada participante. Embora esse método forneça uma visão detalhada, ele pode resultar na perda de dados extremos. Quanto à análise de dados qualitativos, foi empregada parcialmente procedimentos de *Grounded Theory* (GT) (CORBIN; STRAUSS, 2008) para definir nosso protocolo de análise de dados. O principal objetivo foi reduzir a subjetividade inerente à codificação das respostas às questões abertas. Todos os dados foram analisados em pares, com o intuito de minimizar vieses individuais e alcançar consenso quanto às categorias e subcategorias identificadas.

## 6.1 Resumo do Capítulo 6

Este capítulo apresentou a discussão das ameaças à validade, evidenciando as precauções metodológicas adotadas para assegurar a robustez e a confiabilidade dos resultados obtidos. As estratégias de mitigação aplicadas em cada dimensão da validade – construto, interna, externa e de conclusão – foram fundamentais para reduzir potenciais vieses e fortalecer a credibilidade das interpretações. Ainda que algumas limitações inerentes ao delineamento do estudo permaneçam, especialmente relacionadas à representatividade da amostra e à subjetividade presente na análise qualitativa, considera-se que os procedimentos adotados foram adequados ao contexto e aos objetivos da pesquisa. O próximo capítulo apresenta as conclusões e direções para trabalhos futuros.

# 7 CONCLUSÕES E TRABALHOS FUTUROS

Este estudo apresentou uma investigação sobre a conscientização de desenvolvedores de *software* brasileiros sobre privacidade de dados. Para tanto, foi conduzido um questionário com 88 desenvolvedores, com o objetivo de explorar: (i) o conhecimento sobre privacidade de dados, utilizando o modelo KAB; (ii) as percepção sobre a frequência, importância e facilidade de uso de 13 estratégias de privacidade de dados; e (iii) os fatores organizacionais que podem influenciar a adoção e adesão às práticas de privacidade de dados dentro das equipes de desenvolvimento. Os achados fornecem evidências empíricas sobre o contexto brasileiro, destacando o grau de conscientização dos desenvolvedores, suas percepções acerca das estratégias de privacidade e os fatores organizacionais que impactam sua implementação. Tais resultados podem orientar pesquisadores e desenvolvedores que buscam compreender os desafios e benefícios de incorporar a privacidade de dados em projetos de *software* na prática.

Nosso estudo revelou que a maioria dos desenvolvedores de *software* brasileiros apresenta um nível moderado de conhecimento e conscientização sobre privacidade de dados. Embora muitos desenvolvedores reconheçam a importância geral da privacidade, seu conhecimento específico sobre regulamentações legais, como o GDPR, é limitado. Além disso, os desenvolvedores geralmente classificaram estratégias de privacidade de dados, como *Criptografia* e *Controle do usuário*, como importantes e fáceis de usar. No entanto, estratégias como *Anonimização* e *Desativar coleta de dados* foram percebidas como menos utilizadas e um pouco mais complexas de implementar, refletindo uma lacuna entre sua importância reconhecida e a adoção prática.

Adicionalmente, foi identificado que fatores organizacionais, como o porte da empresa, setor de atuação e a presença de um responsável ou equipe dedicada à privacidade, tendem a influenciar a adoção de práticas de privacidade de dados. Organizações maiores e aquelas situadas em setores altamente regulados demonstraram um nível mais

elevado de adesão às estratégias de privacidade de dados. Em contraste, organizações menores frequentemente carecem de recursos ou expertise para implementar plenamente práticas abrangentes de privacidade.

Em conclusão, o estudo destaca a necessidade de treinamento aprimorado e maior conscientização entre desenvolvedores de *software*, particularmente em relação aos requisitos legais e a medidas de privacidade mais avançadas. Além disso, as organizações devem investir em políticas de privacidade claras e alocar recursos suficientes para garantir que a privacidade de dados seja efetivamente integrada ao ciclo de desenvolvimento de *software*. Como trabalhos futuros, propõe-se condução de um estudo longitudinal para avaliar mudanças na conscientização e nas práticas de privacidade, especialmente em resposta a novas regulamentações, bem como a eficácia de diferentes abordagens na redução da lacuna de conscientização sobre privacidade. Adicionalmente, uma investigação sobre como diferenças regionais dentro do Brasil e características organizacionais, como cultura e porte da empresa, podem influenciar a forma como a privacidade é priorizada e apoiada dentro das organizações.

# REFERÊNCIAS

ASHCRAFT, C.; MCLAIN, B.; EGER, E. **Women in tech: The facts**. [S.l.]: National Center for Women & Technology (NCWIT) Colorado, CO, USA, 2016. Disponível em: https://wpassets.ncwit.org/wp-content/uploads/2021/05/13193304/ncwit_women-in-it_2016-full-report_final-web06012016.pdf. Acesso em 3 mar. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. 2018. <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

CALDIERA, V. R. B.-G.; ROMBACH, H. D. Goal question metric paradigm. **Encyclopedia of software engineering**, v. 1, n. 528-532, p. 6, 1994. Disponível em: https://www.cs.umd.edu/ mvz/handouts/gqm.pd. Acesso em 14 mar. 2025.

CANEDO, E. D.; BANDEIRA, I. N.; CALAZANS, A. T. S.; COSTA, P. H. T.; CANÇADO, E. C. R.; BONIFÁCIO, R. Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. **Requir. Eng.**, v. 28, n. 2, p. 177–194, 2023. Disponível em: https://doi.org/10.1007/s00766-022-00382-8. Acesso em 2 mar. 2025.

CANEDO, E. D.; CALAZANS, A. T. S.; CERQUEIRA, A. J.; COSTA, P. H. T.; MASSON, E. T. S. Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In: **Proceedings of the 29th IEEE International Requirements Engineering Conference, RE 2021, Notre Dame, IN, USA, September 20-24, 2021**. [S.l.]: IEEE, 2021. p. 58–69. Disponível em: https://doi.org/10.1109/RE51729.2021.00013. Acesso em 7 mar. 2025.

CHEUNG, M. Y. M.; LIU, H. Information privacy concerns in generative AI. In: **Proceedings of the Australasian Conference on Information Systems, ACIS 2023, Wellington, New Zealand, December 5-8, 2023**. [S.l.: s.n.], 2023. Disponível em: https://aisel.aisnet.org/acis2023/24. Acesso em 2 mar. 2025.

CORBIN, J.; STRAUSS, A. Basics of qualitative research: Techniques and procedures for developing grounded theory. **Thousand Oaks**, v. 3, p. 1–400, 2008. Disponível em: https://archive.org/details/basicsofqualitat0000stra. Acesso em 13 mar. 2025.

DIAS-NETO, A. C.; MATALONGA, S.; SOLARI, M.; ROBIOLO, G.; TRAVASSOS, G. H. Toward the characterization of software testing practices in south america: looking at brazil and uruguay. **Software Quality Journal**, Springer, v. 25, p. 1145–1183, 2017. Disponível em: doi.org/10.1007/s11219-016-9329-3. Acesso em 22 mar. 2025.

FERRÃO, S. É. R.; SILVA, G. R. S.; CANEDO, E. D.; MENDES, F. F. Towards a taxonomy of privacy requirements based on the LGPD and

ISO/IEC 29100. **Inf. Softw. Technol.**, v. 168, p. 107396, 2024. Disponível em: https://doi.org/10.1016/j.infsof.2024.107396. Acesso em: 25 fev. 2025.

FERRARA, E. Should chatgpt be biased? challenges and risks of bias in large language models. **First Monday**, v. 28, n. 11, p. 13346/11369, 2023. Disponível em: https://doi.org/10.5210/fm.v28i11.13346, Acesso em 27 fev. 2025.

FRANKE, L.; LIANG, H.; FARZANEHPOUR, S.; BRANTLY, A.; DAVIS, J. C.; BROWN, C. An exploratory mixed-methods study on general data protection regulation (GDPR) compliance in open-source software. In: FRANCH, X.; DANEVA, M.; MARTÍNEZ-FERNÁNDEZ, S.; QUARANTA, L. (Ed.). **Proceedings of the 18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2024, Barcelona, Spain, October 24-25, 2024**. [S.l.]: ACM, 2024. p. 325–336. Disponível em: https://doi.org/10.1145/3674805.3686692. Acesso em 6 mar. 2025.

GLASER, B.; STRAUSS, A. **Discovery of grounded theory: Strategies for qualitative research**. [S.l.]: Routledge, 2017. Disponível em: https://doi.org/10.4324/9780203793206. Acesso em 15 mar. 2025.

GOLDA, A.; MEKONEN, K.; PANDEY, A.; SINGH, A.; HASSIJA, V.; CHAMOLA, V.; SIKDAR, B. Privacy and security concerns in generative AI: A comprehensive survey. **IEEE Access**, v. 12, p. 48126–48144, 2024. Disponível em: https://doi.org/10.1109/ACCESS.2024.3381611. Acesso em 5 mar. 2025.

GRISSOM, R. J.; KIM, J. J. **Effect sizes for research: A broad practical approach**. [S.l.]: Lawrence Erlbaum Associates Publishers, 2005. Disponível em: https://10.4324/9781410612915. Acesso em 3 mar. 2025.

HADAR, I.; HASSON, T.; AYALON, O.; TOCH, E.; BIRNHACK, M.; SHERMAN, S.; BALISSA, A. Privacy by designers: software developers' privacy mindset. **Empirical Software Engineering**, Springer, v. 23, p. 259–289, 2018. Disponível em: https://doi.org/10.1007/s10664-017-9517-1. Acesso em 23 mar. 2025.

IWAYA, L. H.; BABAR, M. A.; RASHID, A. Privacy engineering in the wild: Understanding the practitioners' mindset, organizational aspects, and current practices. **IEEE Transactions on Software Engineering**, v. 49, n. 9, p. 4324–4348, 2023. Disponível em https://10.1109/TSE.2023.3290237. Acesso em 29 mar. 2025.

JESUS, E. D. B. D.; VILELA, J.; SILVA, C. Requisitos de segurança e privacidade em startups: Um estudo empírico em uma aplicação de governança de dados. In: LUCENA, M.; LENCASTRE, M.; BALLEJOS, L. C. (Ed.). **Anais do WER24 - Workshop em Engenharia de Requisitos, Buenos Aires, Argentina, August 7-9, 2024**. [S.l.]: Even3,

Brasil, 2024. Disponível em: https://doi.org/10.29327/1407529.27-13. Acesso em 2 mar. 2025.

KEMPE, E.; MASSEY, A. Regulatory and security standard compliance throughout the software development lifecycle. In: **Proceedings of the 54th Hawaii International Conference on System Sciences, HICSS 2021, Kauai, Hawaii, USA, January 5, 2021**. [S.l.]: ScholarSpace, 2021. p. 1–10. Disponível em: https://hdl.handle.net/10125/70861. Acesso em 27 fev. 2025.

KITCHENHAM, B.; PFLEEGER, S. L. Principles of survey research: part 5: populations and samples. **ACM SIGSOFT Software Engineering Notes**, ACM, v. 27, n. 5, p. 17–20, 2002. Disponível em: https://10.1145/571681.571686. Acesso em 8 mar. 2025.

KRUGER, H. A.; KEARNEY, W. D. A prototype for assessing information security awareness. **Computers & security**, Elsevier, v. 25, n. 4, p. 289–296, 2006. Disponível em: https://doi.org/10.1016/j.cose.2006.02.008. Acesso em 27 mar. 2025.

KSHETRI, N. Navigating EU regulations: Challenges for U.S. technology firms and the rise of europe's generative AI ecosystem. **Computer**, v. 57, n. 10, p. 112–117, 2024. Disponível em: https://doi.org/10.1109/MC.2024.3433088, Acesso em: 27 fev. 2025.

LANDIS, C. B.; KROLL, J. A. Mitigating inference risks with the NIST privacy framework. **Proc. Priv. Enhancing Technol.**, v. 2024, n. 1, p. 217–231, 2024. Disponível em: https://doi.org/10.56553/popets-2024-0013. Acesso em 1 Mar. 2025.

LESTER, C. Y.; JAMERSON, F. Incorporating software security into an undergraduate software engineering course. In: **Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009, 18-23 June 2009, Athens/Glyfada, Greece**. [S.l.]: IEEE Computer Society, 2009. p. 161–166. Disponível em: https://10.1109/SECURWARE.2009.32. Acesso em 23 mar. 2025.

LIKERT, R. **A Technique for the Measurement of Attitudes**. [S.l.]: Archives of Psychology, 1932. (A Technique for the Measurement of Attitudes, Nº 136-165). Disponível em: https://archive.org/details/likert-1932. Acesso em 10 mar. 2025.

LINÅKER, J.; SULAMAN, S. M.; MELLO, R. M. de; HÖST, M. Guidelines for conducting surveys in software engineering. **Technical report**, Department of Computer Science, Lund University, 2015. Disponível em: https://portal.research.lu.se/en/publications/8ac54dbe-b7ac-4244-9c43-0f0d157efa26. Acesso em 12 mar. 2025.

LITWIN, M. S.; FINK, A. **How to measure survey reliability and validity**. https://methods.sagepub.com/book/how-to-measure-survey-reliability-and-validity: Sage, 1995. v. 7. Disponível em: https://doi.org/10.4135/9781483348957. Acesso em 9 mar. 2025.

MATOS, A.; PATRÍCIO, M.; NICOLAU, M. I.; CANEDO, E. D.; PEREIRA, J. A.; UCHÔA, A. Data privacy in software practice: Brazilian developers' perspectives. **Journal of Internet Services and Applications**, v. 16, n. 1, p. 299–319, 2025. Disponível em: https://doi.org/10.5753/jisa.2025.5302. Acesso em 12 mar. 2025.

PARSONS, K.; MCCORMAC, A.; BUTAVICIUS, M. A.; PATTINSON, M. R.; JERRAM, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). **Comput. Secur.**, v. 42, p. 165–176, 2014. Disponível em: https://doi.org/10.1016/j.cose.2013.12.003. Acesso em 27 mar. 2025.

PEIXOTO, M. M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C.; VILELA, J.; ARAÚJO, J.; GORSCHEK, T. The perspective of brazilian software developers on data privacy. **J. Syst. Softw.**, v. 195, p. 111523, 2023. Disponível em: https://doi.org/10.1016/j.jss.2022.111523. Acesso em 28 fev. 2025.

RALPH, P.; BALTES, S.; ADISAPUTRI, G.; TORKAR, R.; KOVALENKO, V.; KALINOWSKI, M.; NOVIELLI, N.; YOO, S.; DEVROEY, X.; TAN, X. *et al.* Pandemic programming: How covid-19 affects software developers and how their organizations can help. **Empirical software engineering**, Springer, v. 25, p. 4927–4961, 2020. Disponível em: https://doi.org/10.1007/s10664-020-09875-y. Acesso em 6 mar. 2025.

ROCHA, L. D.; SILVA, G. R. S.; CANEDO, E. D. Privacy compliance in software development: A guide to implementing the LGPD principles. In: HONG, J.; LANPERNE, M.; PARK, J. W.; CERNÝ, T.; SHAHRIAR, H. (Ed.). **Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, SAC 2023, Tallinn, Estonia, March 27-31, 2023**. [S.l.]: ACM, 2023. p. 1352–1361. Disponível em: https://doi.org/10.1145/3555776.3577615, Acesso em: 26 fev. 2025.

ROMANO, J.; KROMREY, J. D.; CORAGGIO, J.; SKOWRONEK, J.; DEVINE, L. Exploring methods for evaluating group differences on the nsse and other surveys: Are the t-test and cohen'sd indices the most appropriate choices. In: CITESEER. **Proceedings of the annual meeting of the Southern Association for Institutional Research**. [S.l.], 2006. p. 1–51. Disponível em: https://www.bibsonomy.org/bibtex/29fb28c468a7f6dc911f2389e76d9f7b6/becker. Acesso em 3 mar. 2025.

SALKIND, N. **Exploring Research**. 8th. ed. [S.l.]: Pearson Education, 2012. Disponível em: https://archive.org/details/exploringresearc0000salk_z7v0. Acesso em 19 mar. 2025.

SANGAROONSILP, P.; DAM, H. K.; CHOETKIERTIKUL, M.; RAGKHITWETSAGUL, C.; GHOSE, A. A taxonomy for mining and classifying privacy requirements in issue reports. **Inf. Softw. Technol.**, v. 157, p. 107162, 2023. Disponível em: https://10.1016/J.INFSOF.2023.107162. Acesso em 28 fev. 2025.

SCHRADER, P. G.; LAWLESS, K. A. The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. **Performance Improvement**, Wiley Online Library, v. 43, n. 9, p. 8–15, 2004. Disponível em: https://doi.org/10.1002/pfi.4140430905. Acesso em 26 mar. 2025.

SHAPIRO, S.; WILK, M. An analysis of variance test for normality (complete samples). **Biometrika**, v. 52, n. 3/4, p. 591–611, 1965. Disponível em: https://www.jstor.org/stable/2333709. Acesso em 17 mar. 2025.

STALLINGS, W. **Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices.** [S.l.]: Addison-Wesley Professional, 2019. Disponível em: https://books.google.com.br/books?id=chrCDwAAQBAJ. Acesso em 29 mar. 2025.

TAHAEI, M.; FRIK, A.; VANIEA, K. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In: **Proceedings of the CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021**. [S.l.]: ACM, 2021. p. 693:1–693:15. Disponível em: https://10.1145/3411764.3445768. Acesso em 23 mar. 2025.

THOMSON, M. E.; SOLMS, R. von. Information security awareness: educating your users effectively. **Inf. Manag. Comput. Secur.**, v. 6, n. 4, p. 167–173, 1998. Disponível em: https://doi.org/10.1108/09685229810227649. Acesso em 28 mar. 2025.

União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em 24 mar. 2025.

WHITLEY, E.; BALL, J. Statistics review 6: Nonparametric methods. **Critical care**, Springer, v. 6, p. 1–5, 2002. Disponível em: https://doi.org/10.1186/cc1820. Acesso em 3 mar. 2025.

WOHLIN, C.; RUNESON, P.; HÖST, M.; OHLSSON, M. C.; REGNELL, B.; WESSLÉN, A. **Experimentation in Software Engineering**. [S.l.]: Springer, 2012. Disponível em: https://doi.org/10.1007/978-3-642-29044-2 . Acesso em: 26 fev. 2025. ISBN 978-3-642-29043-5.

# APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Este documento, denominado Termo de Consentimento Livre e Esclarecido (TCLE), visa assegurar seus direitos como participante e será disponibilizado por meio eletrônico. Por favor, leia com atenção e calma, buscando entender completamente a proposta da pesquisa. Não haverá qualquer tipo de penalização ou prejuízo se você não quiser participar ou retirar sua autorização em qualquer momento.

1. **INFORMAÇÕES SOBRE ESTA PESQUISA**
    a) **Objetivos:** O objetivo desta pesquisa consiste em avaliar duas abordagens de ensino e aprendizagem de padrões de segurança e vulnerabilidades de software para sistemas web, no que diz respeito ao seu impacto na motivação e aprendizado dos estudantes.
    b) **Importância do estudo:** Este estudo visa obter *insights* valiosos para promover um ambiente mais seguro em termos de privacidade de dados em software.
    c) **Procedimentos e metodologias:** Para participar desta pesquisa, você precisa ter mais de 18 anos e atuar na área de desenvolvimento de software ou segurança da informação. Sua participação consistirá em responder a um questionário online sobre privacidade de dados no desenvolvimento de sistemas, que levará aproximadamente 15 minutos para ser concluído. A confidencialidade e anonimato dos participantes serão rigorosamente mantidos, incentivando respostas francas e honestas para fornecer *insights* valiosos sobre a temática em questão.
    d) **Tratamento dos dados:** Durante todo o processo, será assegurado o respeito às normas de privacidade e ética, conforme preconizado pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018), garantindo que as informações

dos participantes sejam tratadas com confidencialidade. Os dados coletados por meio do questionário online serão anonimizados, removendo qualquer informação que possa identificar diretamente os participantes. Os dados serão organizados e codificados para facilitar a análise. Os resultados serão apresentados de forma agregada e não identificável individualmente, preservando assim a privacidade dos participantes de acordo com as disposições legais aplicáveis.

e) **Forma de contato com os pesquisadores:** Sempre que desejar, você poderá entrar em contato para obter informações sobre este projeto de pesquisa, sobre sua participação ou outros assuntos relacionados à pesquisa. Aryely Matos (<aryelymatos@alu.ufc.br>) e Maria Isabel Nicolau (<mariaisabel@aluno.puc-rio.br>). Os professores responsáveis peleo estudo são Anderson Uchôa (<andersonuchoa@ufc.br>), Edna Dias Canedo (<ednacanedo@unb.br>) e Juliana Alves Pereira (<juliana@inf.puc-rio.br>).

2. **GARANTIAS AOS PARTICIPANTES**

a) **Direito de recusa a participar:** Sua participação nesta pesquisa é voluntária (sem remuneração e recompensas) e não obrigatória. Você possui plena liberdade para decidir se deseja participar dela, não sofrendo qualquer tipo de penalidade caso opte por não participar.

A qualquer momento, você pode se recusar a participar e se retirar da pesquisa, sem constrangimentos, penalidades ou qualquer prejuízo. As informações e materiais obtidos nesta pesquisa não serão utilizados para outras finalidades que não sejam dentro do contexto desta.

b) **Sigilo e privacidade:** Garantimos a total confidencialidade e anonimato de suas respostas. Todas as informações sensíveis, como nomes de empresas ou de outras pessoas, serão completamente anonimizadas.

c) **Responsabilidade do(a) Pesquisador(a):** Asseguramos fornecer este docu-

mento ao participante da pesquisa e utilizar os dados obtidos exclusivamente para as finalidades descritas neste documento ou conforme o consentimento dado pelo(a) participante.

# APÊNDICE B – *SCRIPT* DO QUESTIONÁRIO

Você está sendo convidado(a) a participar, como voluntário(a), da pesquisa *"Investigando Práticas e Estratégias de Privacy by Design"* realizada pela UFC, UnB e PUC-Rio.

Esta pesquisa tem como objetivo explorar aspectos relacionados à privacidade de dados no processo de desenvolvimento de software desde a concepção. Queremos compreender o nível de consciência dos desenvolvedores sobre o conceito de *Privacy by Design*. Também buscamos entender as práticas relacionadas ao uso de estratégias para garantir privacidade de dados em sistemas. Além disso, estamos interessados em entender como fatores organizacionais podem influenciar a adesão às práticas de privacidade dentro das equipes de desenvolvimento. Ao analisar esses diferentes aspectos, esperamos obter *insights* valiosos para promover um ambiente mais seguro em termos de privacidade de dados em software.

Para participar desta pesquisa, é necessário ter mais de 18 anos e experiência na área de desenvolvimento de software ou segurança da informação. Sua participação consiste em responder a um questionário online sobre privacidade de dados no desenvolvimento de sistemas, que levará aproximadamente 15 minutos para ser concluído. Garantimos o sigilo e a confidencialidade de todas as informações fornecidas durante a pesquisa.

As pesquisadoras responsáveis são: Aryely Matos (<aryelymatos@alu.ufc.br>) e Maria Isabel Nicolau (<mariaisabel@aluno.puc-rio.br>). Os professores responsáveis são Anderson Uchôa (<andersonuchoa@ufc.br>), Edna Dias Canedo (<ednacanedo@unb.br>) e Juliana Alves Pereira (<juliana@inf.puc-rio.br>).

O Termo de Consentimento Livre e Esclarecido (TCLE) visa assegurar seus direitos como participante e está disponível neste link. Por favor, leia-o com atenção para entender completamente a proposta da pesquisa. Sua participação é voluntária, e

você pode optar por não participar ou retirar seu consentimento a qualquer momento, sem qualquer penalização ou prejuízo.

Após ter recebido esclarecimentos sobre a natureza da pesquisa, seus objetivos e métodos, eu declaro que sou maior de 18 anos e aceito participar por meio do formulário de participação, conforme as disposições da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Em caso de resposta negativa, o formulário será encerrado, garantindo assim o respeito à autonomia e privacidade dos participantes, conforme estabelecido pela legislação vigente. (Obrigatória)

( ) Aceito participar

( ) Não aceito participar

**CARACTERIZAÇÃO GERAL DO PARTICIPANTE**

Nesta seção recolheremos informações básicas e dados pessoais para entender um pouco mais sobre o seu perfil.

**Questão 1.** Qual é a sua idade? (Obrigatória)

( ) 18-24 anos

( ) 25-34 anos

( ) 35-44 anos

( ) 45-54 anos

( ) 55-64 anos

( ) 65 anos ou mais

( ) Prefiro não dizer

**Questão 2.** Em qual estado você reside atualmente? (Obrigatória)

( ) Acre (AC)

( ) Alagoas (AL)

( ) Amapá (AP)

( ) Amazonas (AM)

( ) Bahia (BA)

( ) Ceará (CE)

( ) Distrito Federal (DF)

( ) Espírito Santo (ES)

( ) Goiás (GO)

( ) Maranhão (MA)

( ) Mato Grosso (MT)

( ) Mato Grosso do Sul (MS)

( ) Minas Gerais (MG)

( ) Pará (PA)

( ) Paraíba (PB)

( ) Paraná (PR)

( ) Pernambuco (PE)

( ) Piauí (PI)

( ) Rio de Janeiro (RJ)

( ) Rio Grande do Norte (RN)

( ) Rio Grande do Sul (RS)

( ) Rondônia (RO)

( ) Roraima (RR)

( ) Santa Catarina (SC)

( ) São Paulo (SP)

( ) Sergipe (SE)

( ) Tocantins (TO)

( ) Fora do país

**Questão 3.** Qual o seu gênero? (Obrigatória)

( ) Homem

( ) Mulher

( ) Não-binário, gênero queer ou não-conformidade de gênero

( ) Prefiro não responder

( ) Outros:_____

**Questão 4.** Qual é o seu nível de educação formal concluída? (Obrigatória)

( ) Ensino Médio

( ) Ensino Superior

( ) Especialização

( ) Estudante de mestrado

( ) Mestrado

( ) Estudante de doutorado

( ) Doutorado

**Questão 5.** Qual seu modelo de trabalho? (Obrigatória)

( ) Remoto

( ) Híbrido

( ) Presencial

**Questão 6.** Qual papel que melhor descreve suas atividades atuais em projetos de desenvolvimento de software? (Obrigatória)

( ) Cryptographer

( ) Data Scientist

( ) Developer (Backend, frontend, fullstack)

( ) DevOps engineer

( ) Penetration tester

( ) Privacy engineer

( ) Product owner

( ) Project Lead / Project Manager

( ) Requirements Engineer

( ) Security engineer

( ) Solution Architect

( ) Test Manager / Tester

( ) UX/UI designer

**Questão 7.** Por favor, indique a senioridade da posição que ocupa. (Obrigatória)

( ) Estagiário

( ) Júnior (até 5 anos)

( ) Pleno (6 a 9 anos)

( ) Sênior (10+ anos)

**Questão 8.** Quantos anos de experiência você tem em funções relacionadas ao desenvolvimento de software ou TI? (Obrigatória)

---

**Questão 9.** Quais são os sistemas que você trabalha atualmente? (múltiplas escolhas possíveis) (Obrigatória)

[ ] Embedded applications

[ ] Operating Systems

[ ] Desktop applications

[ ] Web applications

[ ] Mobile applications

[ ] Developer tools

[ ] Middleware

[ ] Outros:_____

**Questão 10.** Quais são os domínios dos sistemas que você trabalha atualmente? (múltiplas escolhas possíveis) (Obrigatória)

[ ] Banking/Financial

[ ] Defense & Security

[ ] Education

[ ] Embedded systems in Automotive or Avionics

[ ] Entertainment

[ ] Healthcare

[ ] Insurance

[ ] Logistics

[ ] Oil & Gas

[ ] Sales/E-commerce

[ ] Telecommunication

[ ] Outros:_____

**Questão 11.** Qual o setor da organização para a qual você trabalha atualmente? (Obrigatória)

( ) Administração pública do Distrito Federal

( ) Administração pública estadual

( ) Administração pública federal

( ) Administração pública municipal

( ) Autônomo

( ) Empresa privada

( ) Microempreendedor Individual (MEI)

( ) Organização Não Governamental

( ) Organização sem fins lucrativos

( ) Projetos de pesquisa e desenvolvimento

( ) Startup

( ) Outros:_____

**Questão 12.** Qual o tamanho da empresa para a qual você trabalha atualmente? (Obrigatória)

( ) Até 9 funcionários

( ) De 10 a 49

( ) De 50 a 99

( ) De 100 a 499

( ) De 500 a 999

( ) Mais de 1000

( ) Não sei

**CARACTERIZAÇÃO DA EXPERIÊNCIA COM PRIVACIDADE DE DADOS NO PROCESSO DE DESENVOLVIMENTO DE SOFTWARE**

Nesta seção, gostaríamos de saber sua experiência de trabalho com privacidade de dados em software.

**Questão 13.** Você tem (ou teve) alguma experiência de trabalho relacionada à privacidade no processo de desenvolvimento de software? (Obrigatória)

( ) Eu já trabalhei (ou trabalho) com privacidade no processo de desenvolvimento de software (por exemplo, design, desenvolvimento e testes).

( ) Meu grupo/equipe de desenvolvimento trabalha (ou trabalhou) com privacidade, mas não estou diretamente envolvido em nenhuma tarefa.

( ) Nunca tive experiência direta e nem indireta com privacidade de software

**Questão 14.** Por favor, descreva brevemente a sua experiência com privacidade de dados em software. Em caso negativo, responda que não possui experiência. (Obrigatória)

---

**Questão 15.** Quais são as principais fontes ou métodos que você costuma usar para aprender sobre questões de privacidade relacionadas ao software? (Obrigatória)

[ ] Workshops

[ ] Seminários

[ ] Hackathons

[ ] Palestras

[ ] Documentação e diretrizes

[ ] Treinamento

[ ] Mentoria

[ ] Ferramentas e bibliotecas

[ ] Outros:_____

**Questão 16.** Que tipos de dados pessoais você trata no seu trabalho? (Obrigatória)

[ ] Identificadores básicos de contato (e.g., nomes, e-mails, telefones)

[ ] Identificadores de presença online (e.g., fotos de perfil, IDs de redes sociais)

[ ] Dados de atividades online (e.g., logs, IPs, user agents)

[ ] Dados de rastreamento online (e.g., cookies, RFID)

[ ] Dados de mídia (e.g., gravações de áudio e vídeo)

[ ] Informações financeiras (e.g., dados bancários, cartões)

[ ] Informações de localização (e.g., geolocalização)

[ ] Informações de emprego (e.g., dados de funcionários)

[ ] Identificadores pessoais (e.g., dados fisiológicos, culturais)

[ ] Informações sociais, políticas ou religiosas

[ ] Informações de associação sindical

[ ] Informações biométricas

[ ] Histórico médico

[ ] Informações pessoais íntimas

[ ] Informações legais

[ ] Não trabalho com dados pessoais

[ ] Outros: _____

**CONSCIÊNCIA SOBRE PRIVACIDADE DE DADOS NO PROCESSO DE DE-**

**SENVOLVIMENTO DE SOFTWARE**

Nesta seção, iremos abordar alguns tópicos e afirmações sobre Privacidade de Dados em Software que resumimos baseados na literatura.

Para responder às próximas perguntas, considere a seguinte definição de **Privacidade de Dados no Processo de Desenvolvimento de Software (Privacidade por Design)**:
*"É um conjunto de práticas e medidas que levam em consideração a privacidade de dados de ponta a ponta no processo de desenvolvimento. A proposta é garantir que a privacidade dos dados seja considerada desde o início do desenvolvimento, continuando até a implementação e manutenção do software"*

**Tópico 1: Conhecimento sobre Privacidade de Dados em Software**

As afirmações a seguir estão relacionadas ao conhecimento sobre privacidade por design

**Questão 17.** Forneça abaixo pelo menos cinco palavras na ordem em que lhe vierem à mente quando você pensa em privacidade. (Obrigatória)

Palavra 01: _____

Palavra 02: _____

Palavra 03: _____

Palavra 04: _____

Palavra 05: _____

**Questão 18.** Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco pontos: 1. Discordo totalmente, 2. Discordo, 3. Neutro, 4. Concordo, 5. Concordo totalmente. (Obrigatória)

| Afirmações (7) | 1. Discordo totalmente | 2. Discordo | 3. Neutro | 4. Concordo | 5. Concordo totalmente |
|---|---|---|---|---|---|
| Eu possuo conhecimento sobre as leis de privacidade relevantes (GDPR, LGPD, HIPAA etc.). | | | | | |
| Eu tenho compreensão sólida das leis e regulamentos específicos de privacidade que influenciam meu trabalho. | | | | | |
| Eu participei de treinamentos internos ou workshops sobre segurança e privacidade. | | | | | |
| Eu me esforço para aprender sobre privacidade por iniciativa pessoal. | | | | | |
| Eu reconheço riscos e preocupações relacionados à privacidade de dados em sistemas de software. | | | | | |
| Eu estou ciente das melhores práticas e técnicas para proteger a privacidade dos usuários. | | | | | |
| Eu sei diferenciar entre segurança e privacidade. | | | | | |

**Questão 19.** Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação. (Opcional)

---

**Tópico 2: Atitudes e Sentimentos sobre Privacidade de Dados em Software**

As afirmações a seguir estão relacionadas a atitudes e sentimentos sobre privacidade por design

**Questão 20.** Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco pontos: 1. Discordo totalmente, 2. Discordo, 3. Neutro, 4. Concordo, 5. Concordo totalmente. (Obrigatória)

| Afirmações (8) | 1. Discordo totalmente | 2. Discordo | 3. Neutro | 4. Concordo | 5. Concordo totalmente |
|---|---|---|---|---|---|
| Eu me preocupo com a possibilidade de ser monitorado ou manipulado ao usar aplicativos ou navegar na internet. | | | | | |
| Eu acredito que a privacidade pessoal é um direito fundamental. | | | | | |
| Eu sinto responsabilidade pessoal em proteger a privacidade dos usuários. | | | | | |
| Eu acredito que é importante educar e conscientizar sobre direitos de privacidade. | | | | | |
| Eu me sinto frustrado com a ideia de que a privacidade é inatingível. | | | | | |
| Eu valorizo o consentimento informado dos usuários. | | | | | |
| Eu reconheço que a retenção de dados deve ser limitada ao propósito do sistema. | | | | | |
| Eu considero a privacidade uma responsabilidade compartilhada. | | | | | |

**Questão 21.** Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação. (Opcional)

---

**Tópico 3: Comportamentos e Ações sobre Privacidade de Dados em Software**

As afirmações a seguir estão relacionadas a comportamento e ações sobre privacidade por design

**Questão 22.** Por favor, com base na sua experiência avalie e classifique cada afirmação a seguir em uma escala de cinco pontos: 1. Discordo totalmente, 2. Discordo, 3. Neutro, 4. Concordo, 5. Concordo totalmente. (Obrigatória)

| Afirmações (6) | 1. Discordo totalmente | 2. Discordo | 3. Neutro | 4. Concordo | 5. Concordo totalmente |
|---|---|---|---|---|---|
| Identificar problemas de privacidade é parte importante da minha rotina profissional. | | | | | |
| Quando encontro problemas de privacidade, informo líderes ou equipes responsáveis. | | | | | |
| Eu proponho soluções para problemas de privacidade encontrados. | | | | | |
| Já atuei como defensor de privacidade (“campeão de privacidade”). | | | | | |
| Em conflitos de privacidade com clientes, busco negociar controles de privacidade. | | | | | |
| Já enfrentei pedidos suspeitos de coleta excessiva de dados. | | | | | |

**Questão 23.** Para as afirmações com as quais você discordou totalmente, descreva o motivo da sua classificação. (Opcional)

---

## ESTRATÉGIAS DE IMPLEMENTAÇÃO PARA GARANTIR PRIVACIDADE DE DADOS EM SOFTWARE

Nessa seção, recolheremos informações sobre as estratégias utilizadas para implementar a privacidade por design.

**Questão 24.** Com que frequência você utiliza técnicas e estratégias de privacidade para garantir a proteção de dados pessoais nas seguintes fases de desenvolvimento? (Obrigatória)

| Fase | Nunca | Raramente | Às vezes | Muitas vezes | Sempre |
|---|---|---|---|---|---|
| Análise de requisitos | | | | | |
| Design | | | | | |
| Codificação | | | | | |
| Estudo de viabilidade | | | | | |
| Instalação | | | | | |
| Deploy | | | | | |
| Teste | | | | | |
| Manutenção | | | | | |

Para responder às próximas perguntas, considere a descrição das seguintes estratégias:

- **Criptografia:** É uma técnica usada para proteger informações, tornando-as inacessíveis a pessoas não autorizadas. Ela converte dados legíveis (texto plano) em um formato ilegível (texto cifrado).
- **Minimização da coleta de dados pessoais:** Refere-se à prática de limitar a quantidade de dados pessoais coletados pela organização.
- **Descentralização:** Consiste na distribuição da coleta, armazenamento e processamento de dados em diferentes locais ou sistemas.
- **Soberania de dados:** Baseia-se em respeitar as leis e regulamentações de proteção de dados em diferentes jurisdições.
- **Dados temporais:** Fundamenta-se em utilizar e armazenar dados apenas pelo tempo necessário.
- **Controle do usuário:** Compreende em dar aos usuários controle sobre seus próprios dados, permitindo que eles acessem, modifiquem e excluam suas informações pessoais conforme necessário.
- **Desligar a coleta de dados:** Consiste em fornecer opções para que os usuários possam optar por não participar da coleta de dados, respeitando suas preferências de privacidade.
- **Anonimização:** Inclui remover ou alterar informações de identificação pessoal de forma que os dados não possam ser associados a indivíduos específicos.

- **Ferramentas de classificação de dados:** São sistemas ou softwares utilizados para classificar e catalogar os dados da organização, facilitando o gerenciamento e a identificação de informações sensíveis ou pessoais.
- **Revisões de design e código:** São práticas que garantem que o processo de desenvolvimento esteja de acordo com técnicas que garantam a segurança em meio a todo o processo do desenvolvimento.
- **Gestão de riscos:** Consiste na avaliação e planejamento dos riscos associados ao processamento de dados.
- **Modelagem de fluxo de dados:** É uma técnica utilizada para representar visualmente o movimento de dados dentro de um sistema de informação.
- **Proxy:** Utiliza-se um proxy para todas as solicitações a serviços de terceiros, a fim de ocultar a identidade dos usuários e impedir que terceiros obtenham informações sobre eles.

**Questão 25.** Com que frequência você utiliza ou já utilizou as seguintes estratégias de privacidade? (Obrigatória)

| **Estratégia** | **Nunca** | **Quase nunca** | **Às vezes** | **Quase sempre** | **Sempre** |
|---|---|---|---|---|---|
| Criptografia | | | | | |
| Minimização | | | | | |
| Descentralização | | | | | |
| Soberania de dados | | | | | |
| Dados temporais | | | | | |
| Controle de usuário | | | | | |
| Desligar a coleta de dados | | | | | |
| Anonimização | | | | | |
| Ferramentas de classificação de dados | | | | | |
| Revisões de design e código | | | | | |
| Gestão de riscos | | | | | |
| Modelagem de fluxo de dados | | | | | |
| Proxy | | | | | |

**Questão 26.** Você utiliza alguma estratégia de privacidade por design que não foi citada

na questão anterior, se sim, qual? (opcional)

---

**Questão 27.** Na sua opinião, qual o nível de importância das seguintes estratégias de implementação de privacidade? (Obrigatória)

| **Estratégia** | **Nada importante** | **Pouco importante** | **Neutro** | **Importante** | **Muito importante** |
|---|---|---|---|---|---|
| Criptografia | | | | | |
| Minimização | | | | | |
| Descentralização | | | | | |
| Soberania de dados | | | | | |
| Dados temporais | | | | | |
| Controle de usuário | | | | | |
| Desligar a coleta de dados | | | | | |
| Anonimização | | | | | |
| Ferramentas de classificação de dados | | | | | |
| Revisões de design e código | | | | | |
| Gestão de riscos | | | | | |
| Modelagem de fluxo de dados | | | | | |
| Proxy | | | | | |

**Questão 28.** Para aquelas estratégias no qual você considerou importante, por favor descreva o motivo da sua classificação. (Opcional)

---

**Questão 29.** Ainda sobre as estratégias, como você caracteriza o grau de facilidade ao usá-las? (Obrigatória)

| Estratégia | Extremamente difícil | Um pouco difícil | Razoavelmente fácil | Bastante fácil | Extremamente fácil |
|---|---|---|---|---|---|
| Criptografia | | | | | |
| Minimização | | | | | |
| Descentralização | | | | | |
| Soberania de dados | | | | | |
| Dados temporais | | | | | |
| Controle de usuário | | | | | |
| Desligar a coleta de dados | | | | | |
| Anonimização | | | | | |
| Ferramentas de classificação de dados | | | | | |
| Revisões de design e código | | | | | |
| Gestão de riscos | | | | | |
| Modelagem de fluxo de dados | | | | | |
| Proxy | | | | | |

**FATORES ORGANIZACIONAIS**

Nesta seção, buscamos coletar informações sobre fatores na organização de desenvolvimento de software em que você está atualmente trabalhando ou na qual já trabalhou anteriormente.

**Questão 30.** Em sua organização, existe uma equipe dedicada apenas para lidar com privacidade? (Obrigatória)

( ) Sim, temos uma equipe interna dedicada exclusivamente à privacidade.

( ) Sim, temos uma equipe terceirizada que lida com privacidade.

( ) Não, não temos uma equipe dedicada, lidamos com privacidade de forma ad-hoc.

( ) Outros _____

**Questão 31.** Na sua organização qual a dinâmica de trabalho para lidar com privacidade e proteção de dados? Por favor, descreva brevemente sobre. (Obrigatória)

---

**Questão 32.** Na sua organização é utilizado uma ou mais ferramentas como softwares para lidar com dados privados? Se sim, quais? (Obrigatória)

( ) Enzuzo

( ) OneTrust

( ) BigID

( ) DataGrail

( ) Securiti

( ) Drata

( ) Ketch

( ) Vanta

( ) Não aplicável (desconheço a utilização de ferramentas na minha organização)

( ) Outros _____

**Questão 33.** Qual a sua percepção com relação a prioridade da organização em que você trabalha sobre privacidade e proteção de dados? (Obrigatória)

( ) Não é uma prioridade

( ) Prioridade baixa

( ) Prioridade média

( ) Prioridade alta

( ) Essencial

**Questão 34.** Na sua percepção quais são os maiores desafios das organizações nos próximos anos sobre práticas e regulamentações para proteger melhor os direitos de privacidade dos usuários? (Obrigatória)

---

**Questão 35.** Por favor, Insira o ano atual para mostrar que você não é um bot (Obrigatória)

---

**Questão 36.** Caso você queira receber os resultados desse estudo e participar de uma futura entrevista sobre Privacidade de Dados, por favor, informe seu Email. (Opcional)

---