**ISSN - 3085-5624**

Eixo Temático 2 - Informação, Comunicação e Processos Tecnológicos

# SEGURANÇA DA INFORMAÇÃO: responsabilidade do desenvolvedor *versus* responsabilidade do usuário

# INFORMATION SECURITY: developer responsibility versus user responsibility

**Álvaro de Araújo Santos** - Faculdade da Cidade de Maceió (FACIMA) – *dtialvaro1@gmail.com* – Orcid: 0009-0004-0586-6089

**Vinicius De Luca** - Faculdade da Cidade de Maceió (FACIMA) - *viniciusdeluca3@gmail.com* – Orcid: https://orcid.org/0009-0001-2033-2761

**Anderson Pereira de Lima Jerônimo** – Centro Universitário Mario Pontes Jucá (UMJ) – *limaand@gmail.com* – Orcid: https://orcid.org/0000-0002-7220-4737

**Paulo José Tenório Cavalcante** – Faculdade da Cidade de Maceió (FACIMA) – *paulo.tenorio.cavalcante@gmail.com* – Orcid: https://orcid.org/0000-0002-5161-9773

**Icaro Santos Ferreira** – Centro Universitário Mario Pontes Jucá (UMJ) – *icaro.ferreira@academico.umj.edu.br* – Orcid: 0000-0003-3033-2244

**Ronaldo Ribeiro Fernandes** - Faculdade da Cidade de Maceió (FACIMA) - *ronaldosmo@hotmail.com* – Orcid: https://orcid.org/0009-0009-8259-7018

**Modalidade: Trabalho Completo**

**Resumo:** A segurança da informação é um desafio que exige a colaboração de todos. Este estudo analisa a responsabilidade compartilhada entre profissionais de software e usuários na proteção de dados. Este estudo aprofunda a complexa questão da segurança da informação, investigando o papel dos atores na proteção de dados. Através de uma análise rigorosa de políticas de segurança e de uma pesquisa abrangente com profissionais da área, o trabalho busca identificar as melhores práticas para mitigar vulnerabilidades e promover comportamentos seguros. Os resultados desta pesquisa têm o potencial de informar políticas e práticas de segurança em diversas organizações, contribuindo para um ambiente digital mais seguro.

**Palavras-Chave**: segurança da informação; proteção de dados; responsabilidade desenvolvedor-usuário.

***Abstract:*** *Information security is a challenge that requires everyone's collaboration. This study analyzes the shared responsibility between software professionals and users in data protection. This study delves into the complex issue of information security, investigating the role of actors in data protection. Through a rigorous analysis of security policies and a comprehensive survey of professionals in the field, the work seeks to identify best practices to mitigate vulnerabilities and promote safe behaviors. The results of this research have the potential to inform security policies and practices in various organizations, contributing to a safer digital environment.*

***Keywords****: information security; data protection; developer-user responsibility.*

## 1. INTRODUÇÃO

O avanço tecnológico redefine as interações entre seres humanos e tecnologia, com uma crescente interdependência entre desenvolvedores de software e usuários finais. Essa interação é crucial para a segurança, eficácia e usabilidade dos produtos digitais, definindo as responsabilidades de cada parte envolvida.

Os profissionais da tecnologia da informação, como programadores, têm a responsabilidade de garantir a segurança e confiabilidade do *software* desde sua concepção até sua manutenção contínua, incluindo codificação segura, testes de qualidade e correções rápidas de falhas. Os usuários, por sua vez, devem adotar práticas de segurança, como senhas fortes e atualizações regulares, além de evitar comportamentos de risco, como o *download* de aplicativos de fontes não confiáveis.

Os profissionais devem assegurar a segurança e confiabilidade do *software*, implementando políticas de segurança robustas durante o processo de desenvolvimento para mitigar potenciais ameaças (Howard; Lipner, 2009). A pesquisa também explora abordagens educacionais em segurança da informação, focando na capacitação dos programadores e usuários finais para lidar com desafios de segurança de forma mais eficiente (Kritzinger; von Solms, 2004).

A segurança da informação é crítica na era digital. A responsabilidade pela segurança recai tanto sobre programadores quanto sobre usuários finais (Bishop, 2003). Esses profissionais devem criar programas seguros e livres de vulnerabilidades conhecidas, enquanto usuários devem seguir diretrizes de segurança, manter o software atualizado e evitar práticas arriscadas (Furnell; Clarke, 2012).

A educação em segurança da informação melhora as práticas dos devs (O termo “devs” ou "dev" é uma abreviação de “developers”, que em português significa desenvolvedores.) e usuários. Com instrução adequada, profissionais de *software* podem implementar políticas de segurança mais eficazes e usuários podem ser educados para proteger suas informações (Kritzinger; von Solms, 2004). Este estudo investiga abordagens educacionais e como aplicá-las de forma eficaz.

## 2. DESENVOLVIMENTO

A segurança da informação é essencial na era digital, sendo um conjunto de estratégias para proteger dados, sistemas e redes contra ameaças. Segundo Nakamura e Geus (2002), a informação é um ativo crucial para os negócios e deve ser protegida adequadamente, garantindo integridade, confidencialidade e disponibilidade.

A segurança da informação envolve tanto devs quanto usuários. Desenvolvedores devem implementar medidas de segurança desde a concepção dos sistemas, incluindo codificação segura, identificação e correção de vulnerabilidades, além de manter os produtos atualizados e corrigir falhas de segurança (Fontes, 2006; Zalewski, 2019). A comunicação clara sobre riscos de segurança é vital para aumentar a conscientização do usuário (Balebako *et al*., 2014).

Usuários, por sua vez, precisam adotar práticas seguras, como criação de senhas fortes, evitar phishing e ataques de engenharia social, e usar autenticação de dois fatores (2FA). A falta de atenção pode resultar em roubo de identidade, perdas financeiras e violação de privacidade.

A evolução tecnológica aumentou a geração, armazenamento e compartilhamento de dados sensíveis, tornando-os alvos potenciais para acessos não autorizados. Dados sensíveis, segundo a Lei Geral de Proteção de Dados (LGPD), incluem informações como origem racial, religiosa, opinião política, propriedade intelectual e registros financeiros.

Em resumo, tanto programadores quanto usuários têm responsabilidades cruciais na proteção da informação, seguindo práticas de segurança para minimizar riscos e proteger dados confidenciais.

### 2.1 *Privacy by default* e *privacy by design*

*Privacy by Design* e *Privacy by Default* são conceitos essenciais na segurança da informação. "*Privacy by Design*" integra práticas de privacidade no design inicial do sistema, enquanto "*Privacy by Default*" garante que as configurações padrão do sistema sejam as mais privativas possíveis (Cavoukian, 2010). Esses princípios são fundamentais para melhorar a segurança da informação.

*Privacy by Design* é uma abordagem que considera a privacidade e a proteção de dados desde o início e ao longo de todo o ciclo de vida do desenvolvimento de sistemas, produtos ou serviços. Já o *Privacy by Default* assegura que, por padrão, apenas os dados pessoais necessários para um propósito específico sejam coletados e retidos, com configurações de privacidade configuradas para proporcionar a proteção por padrão.

A análise dos dados sobre responsabilidade na segurança da informação revela uma tendência preocupante entre os profissionais de desenvolvimento de *software*. Apesar do papel crucial dos, apesar do papel crucial dos profissionais na criação de sistemas seguros na criação de sistemas seguros, há uma significativa falta de conhecimento e negligência em práticas de segurança. Cavoukian (2010) destaca que a integração de princípios como *Privacy by Design* e *Privacy by Default* é essencial para mitigar riscos, mas essa abordagem ainda não é amplamente adotada na prática.

Os dados coletados mostram a prevalência de falhas comuns e a frequência com que os programadores não implementam medidas de segurança adequadas, evidenciando a necessidade de melhorias na educação e conscientização sobre segurança da informação entre os profissionais de desenvolvimento de *software*.

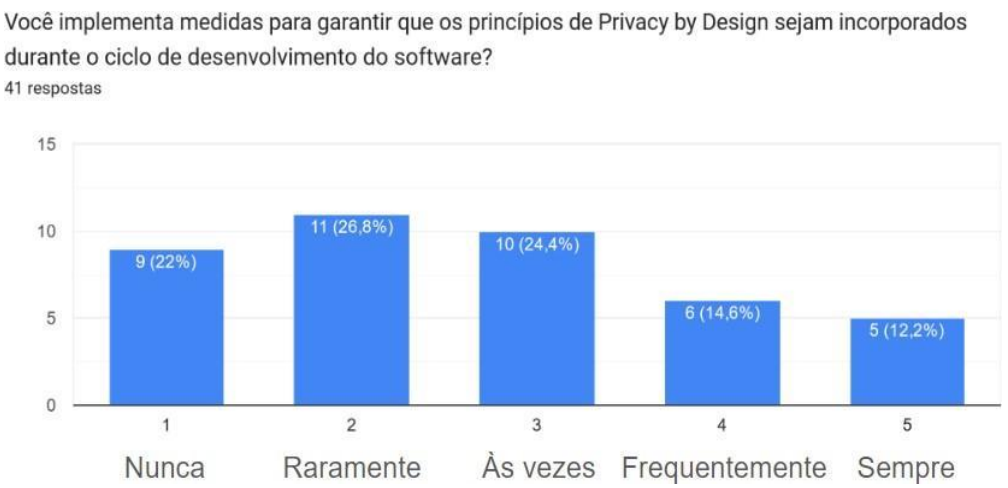
A pesquisa foi realizada através de um estudo de artigos acadêmicos relevantes sobre segurança da informação e incluiu uma pesquisa prática utilizando o *Google Forms*, envolvendo tanto desenvolvedores de *software* quanto usuários comuns.

Gráfico 1 - Familiaridade dos desenvolvedores sobre *Privacy by Design* e *Privacy by Default*.


Fonte: Dados da Pesquisa (2024).

Segundo os resultados apresentados no Gráfico 1, muitos profissionais de tecnologia não possuem familiaridades com os conceitos de *Privacy by Design* e *Privacy by Default*, o que representa a falta de capacitação destes profissionais para desenvolver *softwares* seguros, focados na privacidade dos dados do usuário.

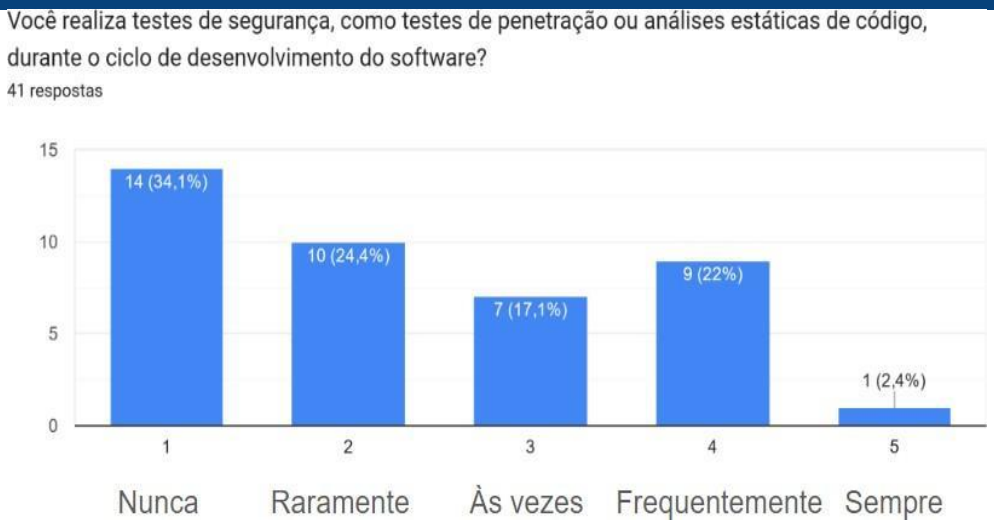
Gráfico 2 - Implementação dos princípios de *Privacy by Design*




Fonte: Dados da Pesquisa (2024).

O Gráfico 2, com os resultados de 1 (nunca) até 5 (sempre), sobre a implementação dos princípios de *Privacy by Design* apresenta uma tendência preocupante, com a maioria das respostas sendo negativas ou neutras, e apenas uma minoria sendo positiva. Isso sugere que muitos programadores ainda não estão priorizando a integração desses princípios desde as fases iniciais do ciclo de desenvolvimento de *software*.

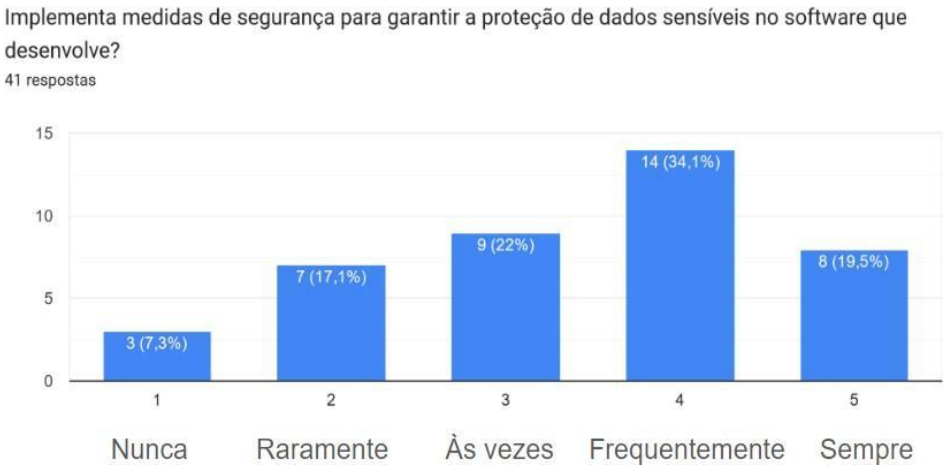
Gráfico 3 - Realizar testes de segurança para garantir a segurança do usuário final




Fonte: Dados da Pesquisa (2024).

O Gráfico 3, com os resultados de 1 (nunca) até 5 (sempre), sobre a realização de testes de segurança para garantir a segurança do usuário final revela uma variedade de respostas, com uma parcela significativa expressando preocupações. Cerca de 34% das respostas foram extremamente negativas, seguidas por 24% negativas e 17% neutras.

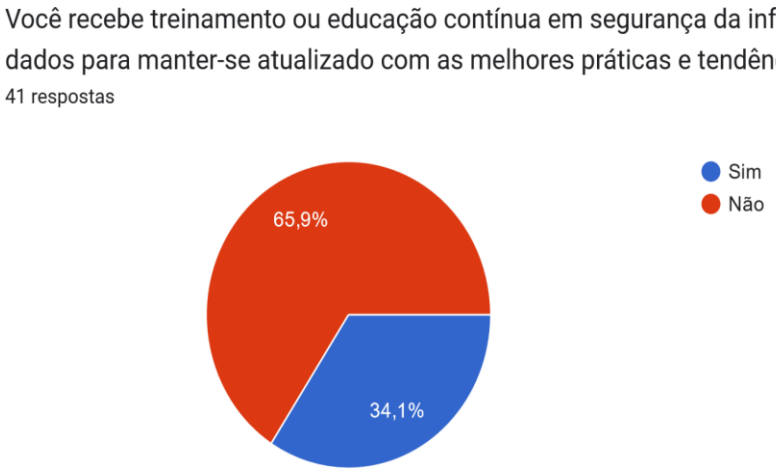
Gráfico 4 - Implementação de proteção a dados sensíveis




Fonte: Dados da Pesquisa (2024).

A proteção de dados sensíveis é uma preocupação central no desenvolvimento de *software*, especialmente em um contexto onde a privacidade dos usuários é cada vez mais valorizada. O Gráfico 4, com os resultados de 1 (nunca) até 5 (sempre), apresenta as percepções dos desenvolvedores em relação à implementação de medidas de proteção de dados sensíveis em seus sistemas.

Gráfico 5 - Treinamento dos desenvolvedores fornecidos pelas empresas

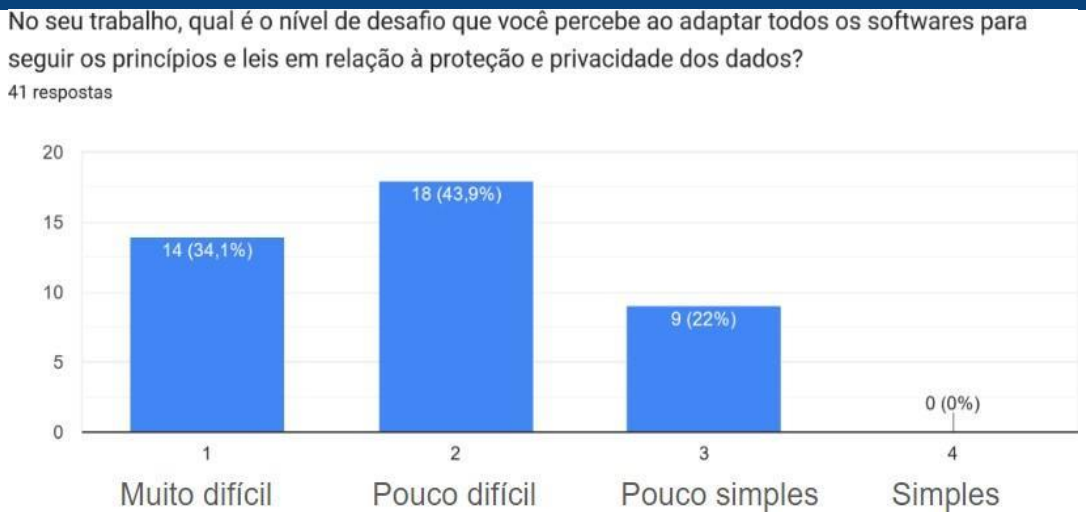



Fonte: Dados da Pesquisa (2024).

Esses resultados destacam a necessidade contínua de conscientização e educação sobre a importância da proteção de dados sensíveis entre os profissionais de *software*, além de enfatizar a urgência de medidas proativas para garantir a conformidade com regulamentações de privacidade, como a LGPD (Lei Geral de Proteção de Dados) no Brasil (Brasil, 2018).

Esses resultados evidenciam a necessidade urgente de investimento em programas de treinamento e conscientização em segurança da informação por parte das empresas, a fim de capacitar seus desenvolvedores na adoção de melhores práticas de desenvolvimento seguro (Acar; Stransky; Wermke *et al*., 2016). A falta de treinamento pode representar uma lacuna significativa na proteção dos sistemas de *software* contra ameaças cada vez mais sofisticadas.

Gráfico 6 - Nível de desafio ao adaptar e seguir os princípios de proteção de privacidade de dados

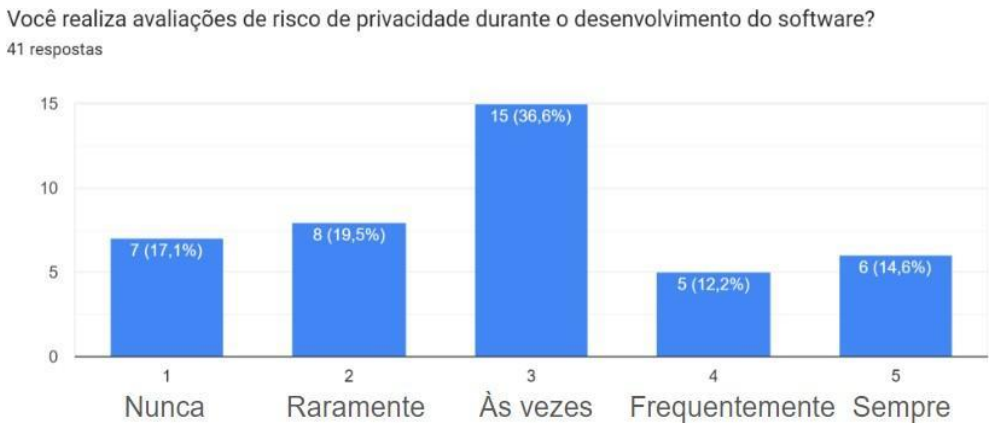



Fonte: Dados da Pesquisa (2024).

É evidente que a maioria das respostas, sendo de 1 (muito difícil) até 4 (simples), reflete uma percepção negativa ou neutra em relação ao desafio de adaptar e seguir os princípios de proteção de privacidade de dados. Essa constatação sugere que os profissionais de tecnologia da informação enfrentam obstáculos significativos ao implementar medidas de privacidade em seus sistemas de *software*.

O Gráfico 7, com os resultados de 1 (nunca) até 5 (sempre), sobre a avaliação de riscos de privacidade no desenvolvimento revela uma distribuição interessante de respostas, com a maioria sendo neutra.

Gráfico 7 - Avaliação de riscos de privacidade no desenvolvimento




Fonte: Dados da Pesquisa (2024).

No entanto, é significativo observar que as respostas se dividem quase igualmente entre muito negativas e muito positivas. Essa diversidade de opiniões sugere uma variedade de abordagens e práticas entre os desenvolvedores em relação à avaliação de riscos de privacidade.

Enquanto alguns podem reconhecer a importância dessa prática e adotá-la de forma proativa, outros podem não considerá-la uma prioridade. Portanto, é fundamental promover uma cultura de conscientização e adoção de práticas robustas de avaliação de riscos de privacidade entre os entre os devs, a fim de garantir a proteção adequada dos dados dos usuários.

## 2.2 Princípios do *privacy by design*

Ann Cavoukian (2011), ao desenvolver o conceito de "*Privacy by Design*" e "*Privacy by Default*", delineou sete princípios fundamentais que orientam a integração da privacidade desde a concepção de sistemas e práticas. Esses princípios são descritos a seguir:

- Proatividade, não reatividade; prevenção, não correção: A abordagem deve ser proativa, antecipando e prevenindo invasões de privacidade antes que ocorram, em vez de reagir a problemas após seu surgimento.
- Privacidade como padrão (*default*): A privacidade deve ser garantida como padrão em qualquer sistema ou prática. Os dados pessoais são protegidos automaticamente, sem que os indivíduos precisem tomar medidas adicionais.
- Privacidade incorporada ao *design*: A privacidade deve ser integrada desde o início ao design de sistemas e práticas, e não adicionada posteriormente como um elemento secundário.
- Funcionalidade total — ganho positivo, não soma zero: A privacidade não deve ser comprometida em troca de outras funcionalidades. Soluções devem ser buscadas para que tanto a privacidade quanto outras necessidades sejam atendidas, resultando em um benefício mútuo.

- Segurança de ponta a ponta — proteção total ao longo do ciclo de vida da informação: A proteção da privacidade deve ser mantida durante todo o ciclo de vida da informação, desde a coleta até o descarte, com medidas de segurança robustas em todas as etapas.
- Visibilidade e transparência — manter o aberto e transparente: As práticas de tratamento de dados devem ser transparentes, permitindo que todas as partes interessadas compreendam como seus dados estão sendo gerenciados, promovendo a responsabilização.
- Respeito pela privacidade do usuário — centrado no usuário: Os interesses e a privacidade dos indivíduos devem ser priorizados. As práticas devem ser projetadas com o usuário em mente, oferecendo configurações claras e acessíveis para a proteção da privacidade.

Esses princípios são essenciais para garantir que a privacidade seja uma consideração central em qualquer desenvolvimento tecnológico ou prática de negócios, promovendo a confiança dos usuários e a conformidade com as regulamentações de privacidade (Cavoukian, 2011).

## 3 CONCLUSÃO

Os resultados obtidos demonstraram que a segurança da informação é uma questão complexa que requer atenção e esforços conjuntos de ambas as partes.

Foi evidenciado que os criadores de software têm um papel crucial na implementação de mecanismos de segurança robustos durante o processo de desenvolvimento do *software*. Eles são responsáveis por garantir que o sistema seja capaz de resistir a ataques maliciosos e proteger as informações dos usuários. No entanto, mesmo com os melhores sistemas de segurança em vigor, a falta de consciência e práticas imprudentes por parte dos usuários podem colocar a segurança da informação em risco.

Os usuários têm a responsabilidade de seguir boas práticas para proteger suas informações pessoais, como usar senhas fortes e atualizadas, evitar clicar em links suspeitos e manter seus sistemas operacionais e *softwares* atualizados. Por outro lado, os profissionais de

desenvolvimento devem fornecer aos usuários as ferramentas necessárias para facilitar essas práticas e educá-los sobre sua importância.

Portanto, conclui-se que a segurança da informação não é uma responsabilidade exclusiva nem dos desenvolvedores nem dos usuários. Em vez disso, é uma colaboração entre ambos para garantir que as informações sejam protegidas efetivamente. Isso sugere uma necessidade cada vez maior de educação em cibersegurança tanto para profissionais técnicos quanto para o público geral.

Os resultados obtidos sugerem que a educação do usuário desempenha um papel crucial na segurança da informação. A falta de compreensão ou negligência dos usuários finais e profissionais de desenvolvimento de *software* em relação às práticas de segurança pode levar à exposição das informações a ataques cibernéticos (Bulgurcu; Cavusogli; Benbasat, 2010). Isso reforça a necessidade de estratégias eficazes de conscientização e treinamento para os usuários, complementando as medidas técnicas implementadas pelos programadores.

## REFERÊNCIAS

ACAR, Y.; STRANSKY, C.; WERMKE, D, *et al*. You Get Where You're Looking for: The Impact of Information Sources on Code Security. *In*: IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP), 1., 2016, San Jose (EUA). **Anais** [...], San Jose (EUA), 2016. p. 289-305.

BALEBAKO, R. **A Survey of Security Advice for Software Developers**. IEEE Security & Privacy, [S.l.], 2014. Disponível em: https://ieeexplore.ieee.org/abstract/document/8077802. Acesso em: 07 jun 2024.

BISHOP, What Is Computer Security?, 2003.

BRASIL**.** Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jun. 2024.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **MIS Quarterly**, Mineápolis, v. 34, 2010, p. 523-548.

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

CAVOUKIAN, A. **Privacy by Design**: The 7 Foundational Principles. Ontario, 2011. Disponível

em: https://www.datatilsynet.no/globalassets/global/bilder/rettigheter-og-plikter/innebygd-personvern/7foundationalprinciples_anncavoukian2.pdf. Acesso em: 14 jun. 2024.

FONTES, E. **Segurança da Informação:** o usuário faz a diferença. 1 ed. São Paulo: Saraiva, 2006.

FURNELL, S.; CLARKE, N. Power to the people? The evolving recognition of human aspects of security. 2012. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404812001228. Acesso em: 17 jun. 2024

HOWARD, M.; LIPNER, S. **The security development lifecycle: SDL: a process for developing demonstrably more secure software**. Microsoft Press, 2009.

KRITZINGER, E.,VON SOLMS, R. **Cyber security for home users:** a new way of protection through awareness enhancement. Computers & Security, 2004.

NAKAMURA, E.; GEUS, P. **Segurança de redes em ambientes corporativos**. São Paulo: Berkeley Brasil, 2002.

ZALEWSKI, M. **Software security:** A guide for project managers. Routledge, 2019.