INTERFACE TECNOLÓGICA

PRIVACIDADE E SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: uma análise dos aspectos psicológicos e cognitivos envolvidos na percepção e na adoção de medidas de segurança

PRIVACY AND SECURITY IN INFORMATION SYSTEMS: An Analysis of the Psychological and Cognitive Aspects Involved in the Perception and Adoption of Security Measures

Jhenifer Fernanda dos Santos – jhenifer.santos09@outlook.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Matão – São Paulo – Brasil

Giuliano Scombatti Pinto – giuliano.pinto@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – São Paulo – Brasil

DOI: 10.31510/infa.v21i1.1979
Data de submissão: 15/04/2024
Data do aceite: 10/03/2024
Data da publicação: 20/06/2024

RESUMO

A proteção da privacidade e segurança em sistemas de informação é um tema cada vez mais relevante na era digital. A rápida evolução da tecnologia trouxe consigo uma infinidade de benefícios, mas também desafios significativos em relação à proteção dos dados pessoais dos usuários. A percepção de segurança em sistemas de informação é influenciada por diversos fatores psicológicos, como a confiança nos sistemas e nas organizações que os operam. Estudos mostram que a confiança é um componente essencial na adoção de medidas de segurança, pois os usuários tendem a adotar comportamentos seguros quando confiam que suas informações serão tratadas de forma adequada e protegidas contra acesso não autorizado. Por outro lado, a desconfiança em relação às práticas de segurança pode levar os usuários a evitar a divulgação de informações pessoais ou a adotar comportamentos de risco, aumentando sua vulnerabilidade a ameaças cibernéticas. O objetivo principal deste estudo é analisar os aspectos psicológicos e cognitivos que influenciam a percepção e adoção de medidas de segurança em sistemas de informação. A metodologia consistiu em uma revisão sistemática da literatura sobre privacidade, segurança e aspectos psicológicos e cognitivos relacionados à percepção e adoção de medidas de segurança em sistemas de informação. Foram utilizadas palavras-chave como "privacidade de dados", "segurança da informação", "psicologia da segurança", "comportamento do usuário" e "tecnologia da informação" para buscar artigos relevantes. A conclusão destaca que a implementação eficaz de medidas técnicas de segurança, conformidade com regulamentações de privacidade e segurança, conscientização dos usuários e comunicação eficaz são essenciais para proteger a privacidade dos dados em sistemas de informação.

Palavras-chave: Privacidade. Segurança. Sistemas de Informação.

ABSTRACT

INTERFACE TECNOLÓGICA

Privacy and security protection in information systems is an increasingly relevant topic in the digital era. The rapid evolution of technology has brought with it a plethora of benefits, but also significant challenges regarding the protection of users' personal data. The perception of security in information systems is influenced by various psychological factors, such as trust in the systems and organizations that operate them. Studies show that trust is a crucial component in the adoption of security measures, as users tend to adopt safe behaviors when they trust that their information will be handled appropriately and protected against unauthorized access. Conversely, distrust in security practices can lead users to avoid disclosing personal information or adopt risky behaviors, increasing their vulnerability to cyber threats. The main objective of this study is to analyze the psychological and cognitive aspects that influence the perception and adoption of security measures in information systems. The methodology consisted of a systematic literature review on privacy, security, and psychological and cognitive aspects related to the perception and adoption of security measures in information systems. Keywords such as "data privacy," "information security," "security psychology," "user behavior," and "information technology" were used to search for relevant articles. The conclusion highlights that the effective implementation of technical security measures, compliance with privacy and security regulations, user awareness, and effective communication are essential to protect data privacy in information systems.

Keywords: Privacy. Security. Information Systems.

1 INTRODUÇÃO

Na sociedade contemporânea, a crescente dependência de sistemas de informação tem gerado uma preocupação crescente com relação à privacidade e segurança. À medida que indivíduos e organizações utilizam esses sistemas para diversos fins, torna-se imperativo compreender os fatores psicológicos e cognitivos que influenciam a percepção e adoção de medidas de segurança. Os sistemas de informação desempenham um papel central nas vidas diárias, desde o armazenamento de informações pessoais até a realização de transações financeiras. No entanto, a confiança nesses sistemas muitas vezes é abalada por preocupações sobre a segurança dos dados e o uso inadequado das informações pessoais. Isso pode levar a uma relutância em adotar medidas de segurança, mesmo quando são disponibilizadas pelos provedores de serviços (Silva, 2021).

Os aspectos psicológicos desempenham um papel significativo na forma como as pessoas percebem o risco e respondem a ele. Por exemplo, indivíduos podem subestimar os riscos de segurança online devido a um otimismo irrealista. Além disso, a falta de compreensão sobre as ameaças potenciais e as medidas de segurança disponíveis pode levar à complacência ou à negação dos problemas de segurança. A cognição também influencia a maneira como as

pessoas lidam com a segurança da informação. Por exemplo, a disponibilidade de certas informações pode influenciar a percepção do risco, com indivíduos atribuindo maior importância a eventos recentes ou amplamente divulgados, mesmo que sejam estatisticamente improváveis. Além disso, a complexidade das medidas de segurança pode dificultar a sua compreensão e adoção por parte dos usuários, especialmente aqueles com menor familiaridade com tecnologia (Ribeiro *et al.*, 2023).

Apesar dos avanços tecnológicos e da implementação de medidas de segurança, violações e vulnerabilidades nos sistemas de informação persistem. Isso levanta a questão: "por que indivíduos e organizações falham em perceber e adotar adequadamente medidas de segurança?". O objetivo principal deste estudo é analisar os aspectos psicológicos e cognitivos que influenciam a percepção e adoção de medidas de segurança em sistemas de informação. Os objetivos específicos incluem:

- Avaliar a eficácia das medidas de segurança técnica na proteção da privacidade dos dados;
- Investigar o impacto das notificações de segurança e alertas sobre o comportamento do usuário;
- Avaliar a eficácia das políticas de privacidade e segurança na influência do comportamento do usuário.

A relevância deste estudo reside em seu potencial para contribuir para o desenvolvimento de estratégias mais eficazes para aprimorar a privacidade e segurança em sistemas de informação. Ao compreender os mecanismos psicológicos e cognitivos subjacentes ao comportamento das pessoas, formuladores de políticas, pesquisadores e profissionais podem projetar intervenções e estratégias direcionadas para enfrentar desafios específicos nesse domínio.

Com base na literatura existente e em estruturas teóricas, as seguintes hipóteses são propostas: (i) indivíduos com níveis mais altos de susceptibilidade percebida a ameaças de segurança têm maior probabilidade de adotar medidas de segurança; (ii) a confiança nos sistemas de informação e instituições influencia positivamente a adoção de medidas de segurança; e (iii) vieses cognitivos, como a heurística da disponibilidade e o viés de otimismo, afetam a percepção de risco e tomada de decisão das pessoas em relação às medidas de segurança.

Este estudo utilizou uma abordagem metodológica bibliográfica. Foi realizada uma revisão sistemática da literatura disponível sobre privacidade, segurança e aspectos

psicológicos e cognitivos relacionados à percepção e adoção de medidas de segurança em sistemas de informação. A pesquisa bibliográfica foi conduzida em bases de dados acadêmicas, como PubMed, Scopus e Web of Science, utilizando palavras-chave: Privacidade, Segurança e Sistemas de Informação, relevantes para identificar estudos relevantes publicados em periódicos científicos, livros e outros recursos pertinentes. A análise dos dados consistiu na seleção, leitura crítica e síntese dos estudos encontrados, visando identificar tendências, lacunas de conhecimento e perspectivas para futuras pesquisas.

Por meio de uma análise abrangente dos aspectos psicológicos e cognitivos envolvidos na percepção e adoção de medidas de segurança em sistemas de informação, este estudo visa fornecer informações para formuladores de políticas, pesquisadores e profissionais. Ao entender os impulsionadores subjacentes do comportamento nesse domínio, é possível desenvolver intervenções e estratégias direcionadas para aprimorar a privacidade e segurança, contribuindo assim para o avanço da tecnologia da informação e da sociedade como um todo.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Eficácia das medidas de segurança técnica na proteção da privacidade dos dados

A eficácia das medidas de segurança técnica na proteção da privacidade dos dados é crucial na era digital, onde a coleta, armazenamento e transmissão de informações pessoais ocorrem em larga escala. Essas medidas técnicas desempenham um papel fundamental na garantia de que os dados sensíveis dos usuários e das organizações permaneçam confidenciais e protegidos contra acesso não autorizado ou violações de segurança. Além disso, a criptografia é uma das medidas mais eficazes para proteger a privacidade dos dados. Ela envolve a conversão de dados em um formato ilegível por meio de algoritmos criptográficos. Mesmo que os dados sejam interceptados durante a transmissão, eles permanecem ininteligíveis para qualquer pessoa sem a chave de descriptografia adequada. A implementação adequada de criptografia em sistemas de informação pode garantir a confidencialidade dos dados, impedindo que terceiros não autorizados os acessem (Silva, 2021).

Ribeiro *et al.* (2023) afirmam que os firewalls são ferramentas essenciais para proteger redes de computadores contra acesso não autorizado. Eles atuam como uma barreira entre a rede interna e externa, filtrando o tráfego de dados com base em regras de segurança predefinidas. Além disso, os controles de acesso, como autenticação de usuário e autorização

de acesso, ajudam a garantir que apenas indivíduos autorizados tenham permissão para acessar determinados dados ou recursos do sistema. Ademais, os sistemas de detecção de intrusão (IDS) e prevenção de intrusão (IPS) monitoram e analisam o tráfego de rede em busca de atividades suspeitas que possam indicar tentativas de acesso não autorizado ou comportamento malicioso. Eles podem identificar e responder a ameaças em tempo real, bloqueando ou neutralizando ataques antes que causem danos significativos aos sistemas e dados.

A proteção de endpoint engloba uma variedade de medidas de segurança destinadas a proteger dispositivos individuais, como computadores, smartphones e tablets, contra ameaças cibernéticas. Isso inclui a instalação de software antivírus, antimalware e firewall pessoal, bem como a implementação de políticas de segurança, como atualizações regulares de software e restrições de acesso. Além disso, a segurança das redes sem fio é essencial para proteger a privacidade dos dados transmitidos por meio de conexões Wi-Fi. Isso envolve a implementação de protocolos de criptografia, como WPA2, para proteger a comunicação entre dispositivos e pontos de acesso sem fio, bem como a configuração adequada de senhas e a segmentação da rede para limitar o acesso a dispositivos autorizados (Soares; Araújo; De Souza, 2020).

Em resumo, Santos e Silva (2023) afirmam que as medidas de segurança técnica desempenham um papel vital na proteção da privacidade dos dados em sistemas de informação. A implementação adequada dessas medidas ajuda a garantir que os dados sensíveis permaneçam confidenciais e protegidos contra ameaças cibernéticas, proporcionando tranquilidade tanto para os usuários quanto para as organizações que lidam com informações pessoais.

As medidas de segurança técnica desempenham um papel crucial na proteção da privacidade dos dados em sistemas de informação. Uma dessas medidas é a criptografia, que consiste na conversão de dados em um formato ilegível por meio de algoritmos criptográficos, garantindo que, mesmo se os dados forem interceptados, permaneçam ininteligíveis sem a chave de descriptografia apropriada. Além disso, firewalls e controles de acesso ajudam a filtrar o tráfego de dados com base em regras de segurança predefinidas, garantindo que apenas usuários autorizados tenham acesso a determinadas informações. Sistemas de detecção e prevenção de intrusões monitoram o tráfego de rede em busca de atividades suspeitas, enquanto medidas de proteção de endpoint, como antivírus e firewall pessoal, protegem dispositivos individuais contra ameaças cibernéticas (Silva, 2021).

A manutenção de sistemas e software atualizados com as últimas correções de segurança é crucial para proteger a privacidade dos dados. As atualizações e patches de segurança são

disponibilizados para corrigir vulnerabilidades conhecidas que podem ser exploradas por hackers. Além disso, auditorias de segurança e monitoramento contínuo dos sistemas de informação ajudam a identificar e corrigir possíveis vulnerabilidades. Em caso de incidentes de segurança, planos de resposta a incidentes e recuperação de desastres bem definidos são essenciais para conter e mitigar os danos (Santos; Silva, 2023).

Soares, Araújo e De Souza (2020) afirmam que o cumprimento das regulamentações de privacidade e segurança, como o GDPR (General Data Protection Regulation) na União Europeia e a LGPD (Lei Geral de Proteção de Dados) no Brasil, é fundamental para evitar penalidades legais e proteger a privacidade dos dados. Isso envolve a implementação de controles e práticas de segurança em conformidade com os requisitos regulamentares aplicáveis. Além disso, a educação e conscientização dos usuários sobre as melhores práticas de segurança da informação são essenciais. Treinamentos regulares, políticas de segurança e incentivos para adoção de comportamentos seguros ajudam a garantir a colaboração dos usuários na proteção da privacidade dos dados. Em suma, a eficácia das medidas de segurança técnica na proteção da privacidade dos dados depende não apenas da implementação adequada dessas medidas, mas também de práticas contínuas de monitoramento, atualização e conformidade, juntamente com a conscientização e colaboração dos usuários.

2.2 Impacto das notificações de segurança e alertas sobre o comportamento do usuário

As notificações de segurança e alertas têm um impacto significativo no comportamento do usuário em relação à segurança da informação. Quando os usuários são alertados sobre potenciais ameaças à segurança de seus dados, isso pode influenciar suas ações e atitudes de várias maneiras. Primeiramente, as notificações aumentam a conscientização dos usuários sobre possíveis ameaças à segurança de seus dados, lembrando-os da importância de estar atento às práticas de segurança e de adotar medidas proativas para proteger suas informações pessoais. Além disso, essas notificações fornecem informações relevantes sobre possíveis riscos e ameaças à segurança, capacitando os usuários a tomarem decisões informadas sobre como agir, como atualizar software, alterar senhas ou evitar determinados comportamentos de risco. Em muitos casos, as notificações também levam os usuários a alterarem seu comportamento online, incluindo a adoção de práticas de segurança adicionais, como o uso de senhas mais fortes ou a ativação da autenticação de dois fatores (Santos; Silva, 2023).

O alerta dos usuários sobre possíveis ameaças à segurança, as notificações ajudam a reduzir os riscos de violações de segurança e comprometimento de dados. Isso ocorre porque os usuários estão mais propensos a agir rapidamente para mitigar os riscos após receberem um alerta de segurança confiável. Além disso, as organizações que fornecem notificações de segurança regulares demonstram um compromisso com a proteção dos dados de seus usuários, aumentando sua confiabilidade e credibilidade aos olhos dos usuários (Ribeiro *et al.*, 2023).

No entanto, Silva (2021) afirma que é importante que as notificações de segurança sejam claras, relevantes e oportunas. Notificações excessivas ou irrelevantes podem levar à fadiga do alerta, fazendo com que os usuários ignorem ou negligenciem avisos importantes. Portanto, é essencial que as organizações projetem suas notificações de segurança de forma apropriada, equilibrando a urgência das informações com a necessidade de evitar sobrecarregar os usuários com alertas desnecessários. Em resumo, as notificações de segurança e alertas desempenham um papel crucial na promoção de comportamentos seguros dos usuários e na proteção da privacidade e segurança dos dados.

2.3. Eficácia das políticas de privacidade e segurança na influência do comportamento do usuário

As políticas de privacidade e segurança desempenham um papel fundamental na influência do comportamento do usuário em relação à proteção de dados pessoais. No contexto jurídico, essas políticas são instrumentos essenciais para estabelecer diretrizes e obrigações tanto para as organizações quanto para os usuários em relação ao tratamento de informações pessoais. A eficácia dessas políticas depende de diversos fatores, incluindo sua clareza, transparência, acessibilidade e adequação às regulamentações vigentes (Custódia, 2016).

Em um estudo realizado por Silveira (2019) foi observado que a compreensão e aceitação das políticas de privacidade e segurança por parte dos usuários são influenciadas por vários elementos, tais como linguagem acessível, apresentação clara das informações, e a percepção dos benefícios e riscos envolvidos. Políticas de privacidade complexas ou excessivamente longas podem resultar em uma falta de compreensão por parte dos usuários, levando-os a ignorar ou rejeitar tais políticas sem uma avaliação adequada.

Além disso, a conformidade das políticas de privacidade e segurança com regulamentações específicas, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia ou a Lei Geral de Proteção de Dados (LGPD) no Brasil, é crucial para garantir

sua eficácia jurídica. Organizações que não cumprem essas regulamentações podem estar sujeitas a penalidades significativas, incluindo multas financeiras e danos à reputação. No entanto, a mera existência de políticas de privacidade e segurança não é suficiente para influenciar o comportamento do usuário. Estudos indicam que a confiança nas organizações e sistemas de informação desempenha um papel crucial na aceitação e adesão às políticas de privacidade e segurança (Calisto *et al.*, 2023). Quando os usuários confiam nas organizações para proteger seus dados pessoais e acreditam que suas informações serão tratadas de forma adequada e segura, eles tendem a ser mais receptivos às políticas de privacidade e segurança propostas (Farias, 2020).

Portanto, observa-se que as políticas de privacidade e segurança têm um impacto significativo no comportamento do usuário em relação à proteção de dados pessoais. Sua eficácia depende não apenas de sua conformidade com regulamentações jurídicas, mas também de sua clareza, transparência e da confiança que inspiram nos usuários. Em um contexto jurídico, é fundamental que as organizações desenvolvam e implementem políticas de privacidade e segurança que atendam aos requisitos legais e promovam a confiança e conformidade por parte dos usuários (Finkelstein; Finkelstein, 2020).

3 PROCEDIMENTOS METODOLÓGICOS

A metodologia da pesquisa consistiu em uma revisão sistemática da literatura sobre privacidade, segurança e aspectos psicológicos e cognitivos relacionados à percepção e adoção de medidas de segurança em sistemas de informação. Utilizaram-se as seguintes palavras-chave para pesquisa: "privacidade de dados", "segurança da informação", "psicologia da segurança", "comportamento do usuário" e "tecnologia da informação".

A pesquisa inicial resultou em 35 artigos potencialmente relevantes. Esses artigos foram então submetidos a critérios de inclusão e exclusão para selecionar os mais pertinentes para a análise detalhada. Após essa etapa, 12 artigos foram selecionados para a revisão crítica e síntese dos resultados. A análise dos dados desses artigos permitiu identificar tendências, lacunas de conhecimento e perspectivas para futuras pesquisas.

Cada um desses estudos foi submetido a uma leitura crítica para avaliar sua relevância, qualidade e contribuição para o campo de estudo. Durante essa etapa, foram identificados diferentes temas e tendências, incluindo a influência da confiança nos sistemas de informação,

os efeitos das notificações de segurança no comportamento do usuário e os vieses cognitivos na percepção de risco.

A análise dos dados resultou na identificação de várias descobertas importantes. Por exemplo, descobriu-se que a confiança nos sistemas de informação influencia positivamente a adoção de medidas de segurança, com uma correlação significativa entre confiança e comportamento seguro. Além disso, notou-se que as notificações de segurança desempenham um papel crucial na conscientização dos usuários sobre possíveis ameaças, levando a mudanças comportamentais em relação à segurança da informação.

4 RESULTADOS E DISCUSSÃO

Os resultados da pesquisa indicam que as medidas de segurança técnica, como criptografia, firewalls e proteção de endpoint, desempenham um papel crucial na proteção da privacidade dos dados em sistemas de informação. Essas medidas foram identificadas como componentes essenciais para garantir a confidencialidade dos dados e protegê-los contra ameaças cibernéticas. Além disso, a conformidade com regulamentações de privacidade e segurança, juntamente com a educação e conscientização dos usuários, foram destacadas como práticas importantes para fortalecer a segurança da informação (Soares; Araújo; De Souza, 2020).

As notificações de segurança e alertas também foram consideradas eficazes para aumentar a conscientização dos usuários sobre potenciais ameaças e influenciar seu comportamento em relação à segurança da informação. No entanto, é crucial que essas notificações sejam claras, relevantes e oportunas para evitar a fadiga do alerta e garantir uma resposta adequada dos usuários. Em resumo, os resultados sugerem que uma abordagem integrada, que combine medidas técnicas de segurança com políticas de conformidade, educação do usuário e comunicação eficaz, é essencial para garantir a proteção eficaz da privacidade dos dados em sistemas de informação. Ao entender os impulsionadores subjacentes do comportamento dos usuários e identificar estratégias para promover comportamentos seguros, é possível desenvolver intervenções e políticas mais eficazes para mitigar os riscos de segurança e proteger as informações pessoais dos usuários (Silva, 2021).

Santos e Silva (2023) afirmam em sua pesquisa que há implicações significativas no âmbito jurídico, especialmente no contexto das regulamentações de privacidade e segurança de dados, como o GDPR na União Europeia e a LGPD no Brasil. Eles destacam a importância da

implementação de medidas técnicas de segurança, conformidade com regulamentações e conscientização dos usuários para garantir a proteção eficaz da privacidade dos dados em sistemas de informação. No contexto jurídico, a eficácia das medidas técnicas de segurança, como criptografia, firewalls e proteção de endpoint, pode ser vista como uma parte essencial do dever de cuidado que as organizações têm para com os dados pessoais dos usuários. A falta de implementação adequada dessas medidas pode resultar em violações de regulamentações de privacidade, sujeitando as organizações a sanções legais significativas.

Além disso, a conscientização dos usuários sobre práticas de segurança da informação e a importância das notificações de segurança e alertas também são aspectos juridicamente relevantes. Organizações que não fornecem informações claras e oportunas sobre possíveis ameaças à segurança dos dados podem ser consideradas negligentes em seus deveres de proteger a privacidade dos usuários. Portanto, do ponto de vista jurídico, os resultados da pesquisa destacam a necessidade de uma abordagem holística para garantir a conformidade com regulamentações de privacidade e segurança de dados. Isso inclui não apenas a implementação de medidas técnicas de segurança, mas também a adoção de políticas de conformidade, educação dos usuários e comunicação eficaz sobre questões de segurança da informação. Essas práticas são essenciais para mitigar os riscos de violações de dados e proteger os direitos de privacidade dos indivíduos no ambiente digital (Ribeiro *et al.*, 2023).

5 CONCLUSÃO

Com base nos resultados obtidos, pode-se concluir que a proteção eficaz da privacidade dos dados em sistemas de informação requer uma abordagem abrangente que englobe tanto medidas técnicas de segurança quanto aspectos jurídicos e comportamentais dos usuários. As medidas de segurança técnica, como criptografia, firewalls e proteção de endpoint, são fundamentais para garantir a confidencialidade dos dados e protegê-los contra ameaças cibernéticas. No entanto, a conformidade com regulamentações de privacidade e segurança, juntamente com a conscientização e educação dos usuários, são igualmente importantes para fortalecer a segurança da informação.

As notificações de segurança e alertas desempenham um papel crucial na conscientização dos usuários sobre possíveis ameaças e na influência de seu comportamento em relação à segurança da informação. No entanto, é essencial que essas notificações sejam claras, relevantes e oportunas para evitar a fadiga do alerta e garantir uma resposta adequada

dos usuários. No âmbito jurídico, os resultados destacam a importância da implementação adequada de medidas técnicas de segurança, conforme exigido por regulamentações como o GDPR na União Europeia e a LGPD no Brasil. Além disso, a conscientização dos usuários e a comunicação eficaz sobre questões de segurança da informação são aspectos juridicamente relevantes, pois organizações que não cumprem suas obrigações de proteger a privacidade dos usuários podem estar sujeitas a sanções legais.

Em suma, a pesquisa enfatiza a necessidade de uma abordagem integrada que combine medidas técnicas de segurança, conformidade regulatória, educação do usuário e comunicação eficaz para garantir a proteção eficaz da privacidade dos dados em sistemas de informação. Ao entender os fatores que influenciam o comportamento dos usuários e identificar estratégias para promover comportamentos seguros, é possível mitigar os riscos de segurança e proteger as informações pessoais dos usuários de forma mais eficaz.

Além disso, os resultados da pesquisa têm implicações importantes no âmbito jurídico, destacando a necessidade de uma abordagem proativa das organizações em relação à proteção da privacidade dos dados. A implementação de medidas técnicas de segurança, como criptografia e firewalls, pode ser vista como parte integrante do dever de cuidado que as organizações têm para com os dados pessoais dos usuários. A falta de implementação adequada dessas medidas pode resultar em violações de regulamentações de privacidade, sujeitando as organizações a sanções legais significativas.

A conscientização dos usuários sobre práticas de segurança da informação e a importância das notificações de segurança e alertas também são aspectos juridicamente relevantes. Organizações que não fornecem informações claras e oportunas sobre possíveis ameaças à segurança dos dados podem ser consideradas negligentes em seus deveres de proteger a privacidade dos usuários. Portanto, do ponto de vista jurídico, os resultados da pesquisa destacam a necessidade de uma abordagem holística para garantir a conformidade com regulamentações de privacidade e segurança de dados.

Essa abordagem holística deve incluir não apenas a implementação de medidas técnicas de segurança, mas também a adoção de políticas de conformidade, educação dos usuários e comunicação eficaz sobre questões de segurança da informação. Essas práticas são essenciais para mitigar os riscos de violações de dados e proteger os direitos de privacidade dos indivíduos no ambiente digital. Portanto, conclui-se que a proteção eficaz da privacidade dos dados em sistemas de informação requer uma abordagem multifacetada que leve em consideração tanto aspectos técnicos quanto jurídicos e comportamentais. Ao adotar essa abordagem integrada, as

organizações podem fortalecer sua postura de segurança da informação e garantir a proteção adequada dos dados pessoais dos usuários em conformidade com as regulamentações aplicáveis.

REFERÊNCIAS

CALISTO, Allan de Aguiar et al. **A influência do design informativo e a visualização de dados aplicados à experiência do usuário em sistemas de recomendação de plataformas de streaming**. 2023.

CUSTÓDIA, Pedro Afonso Vial da. **Política de privacidade nas mídias sociais: termos e condições de uso do Facebook e do Google+ no Brasil**. 2016.

FARIAS, Thalyta Soares de. **Privacidade, monetização de dados pessoais e a LGPD: desafios e impactos da Lei Nº 13.709/2018**. 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. **Privacidade e lei geral de proteção de dados pessoais**. Revista de Direito Brasileira, v. 23, n. 9, p. 284-301, 2020.

RIBEIRO, Sueny Léda Araújo et al. **Comportamento humano em segurança da informação: estudo aplicado às Universidades Federais do Brasil**. 2023.

SANTOS, Rogério Batista dos; SILVA, Tiago Barros Pontes. **Gestão da segurança da informação e comunicações análise ergonômica para avaliação de comportamentos inseguros**. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, v. 19, p. e021024, 2023.

SILVA, Simone de Assis Alves da. **Privacidade de dados e regime de informação: uma análise da plataforma Facebook Business**. 2021. Tese de Doutorado. Doutorado em Sistemas de Informação e Gestão do Conhecimento.

SILVEIRA, Jonas Rafael et al. Segurança da Informação**: Uma análise da percepção de ameaças que influenciam a Intenção de Cumprir as Políticas de Segurança da Informação por usuários de organizações do estado do Rio Grande do Sul**. Revista de Tecnologia Aplicada, v. 8, n. 1, 2019.

SOARES, Hebert Junior; ARAÚJO, Nelcileno V. de S.; DE SOUZA, Patricia. **Privacidade e Segurança Digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade**. In: Anais do I Workshop sobre as Implicações da Computação na Sociedade. SBC, 2020. p. 97-106.