Segurança Digital: Vazamento de Dados e Seus Impactos na Vida dos Usuários

Ulisses Gabriel de Lima Pinheiro[1], Maria Isabelly Soares da Silva[1], Clara Heloisa Cerqueira Fonseca[1], Camilla Priscilla Oliveira dos Santos[1], Rodrigo Siqueira Martins[1], Diego da Silva Pereira[1]

[1] Laboratório de Pesquisa em Redes e Sistemas Computacionais (NOCS LAB), Instituto Federal do Rio Grande do Norte, Parnamirim, Brasil (ulisses.pinheiro@escolar.ifrn.edu.br)

Resumo: A Segurança Digital tornou-se um tema essencial dentro da sociedade devido ao crescimento do uso da internet e do armazenamento de informações pessoais em plataformas digitais. Dentro desse contexto, os vazamentos desses dados armazenados têm se tornado algo cada vez mais frequentes, resultando em uma exposição de informações sensíveis de milhões de pessoas e provocando infinitos prejuízos. Este estudo tem como objetivo analisar os impactos que os vazamentos causam na vida dos usuários, destacando suas principais causas e formas de prevenção. A pesquisa foi desenvolvida através de revisão bibliográfica, utilizando artigos, notícias e outros materiais relacionados à segurança digital e à proteção de dados. Os resultados apontam que os vazamentos têm a capacidade de causar prejuízos financeiros, roubo de identidade, danos emocionais, perda da privacidade e, claro, a exposição indevida das informações pessoais vazadas. Ademais, identificou-se que fatores como ataques hackers, descuidos humanos e debilidade nos sistemas colaboram de forma significativa para esses incidentes. Assim, verifica-se que a conscientização sobre o assunto, unida à medidas de proteção, como senhas fortes, autenticação de dois fatores e atualização frequente dos sistemas, é primordial para reduzir os riscos de outros incidentes e proteger os usuários no espaço digital.

Palavras-chave: *Segurança digital; Vazamento de dados; Proteção de dados; Cibersegurança.*

INTRODUÇÃO

Nos últimos anos, a evolução da tecnologia e a forma como o uso da internet não só cresceu, como também se modificou, transformou por completo a maneira que as pessoas se comunicam, trabalham e guardam suas informações pessoais. Na atualidade, uma grande parte da população usufrui de plataformas digitais todos os dias para todo tipo de atividade, principalmente financeiras, compartilhando dados sensíveis como números de documentos, senhas e informações bancárias com uma frequência sem precedentes. No entanto, juntamente ao avanço tecnológico, também houve um aumento significativo nos casos de ataques cibernéticos e vazamentos de dados pessoais. O Brasil, inclusive, figura entre os países mais afetados por esse tipo de incidente no mundo, o que evidencia a fragilidade da infraestrutura de segurança digital adotada por empresas e órgãos públicos. Segundo Almeida e Soares (2022), a era digital trouxe novas dinâmicas em que "a informação como um bem valioso, e sua proteção, uma prioridade".

Ainda nesse contexto, a segurança digital tornou-se primordial para a proteção das informações pessoais e para a prevenção de golpes, vazamentos e invasões. De acordo com Oliveira e Novais (2024), "o vazamento de dados pessoais pode levar a consequências graves, como roubo de identidade", além de fraude financeira, a prejuízos emocionais às vítimas e a exposição desses dados que podem comprometer a privacidade, a segurança e o bem-estar dos indivíduos, contribuindo para o aumento da sensação de insegurança no ambiente digital. Diante desse cenário, justifica-se a relevância desse estudo, uma vez que a compreensão dos riscos e das medidas de proteção disponíveis pode contribuir tanto para a conscientização individual dos usuários quanto para a melhoria das práticas de segurança adotadas por empresas e instituições. Dessa forma, discutir a importância da segurança digital tornou-se fundamental diante dos riscos presentes na internet. Assim, este trabalho tem como objetivo investigar os impactos dos vazamentos de dados na vida dos usuários, compreender a importância da segurança digital na proteção das informações pessoais, apresentar medidas de proteção e prevenção digital e analisar as principais causas dos vazamentos de dados e seus efeitos sobre os usuários.

MATERIAL E MÉTODOS

Para compreender os impactos dos vazamentos de dados na rotina dos usuários, este estudo utilizou uma abordagem mista (qualitativa e quantitativa). Essa escolha fundamenta-se em Creswell (2010), que destaca que a combinação dessas abordagens permite uma compreensão mais ampla do problema de pesquisa. O estudo foi estruturado em duas etapas complementares: teórica e prática.

A etapa teórica consistiu em pesquisa bibliográfica em bases de dados científicas e normativas, abordando conceitos relacionados à segurança da informação e à proteção de dados pessoais, com destaque para a Lei Geral de Proteção de Dados (LGPD).

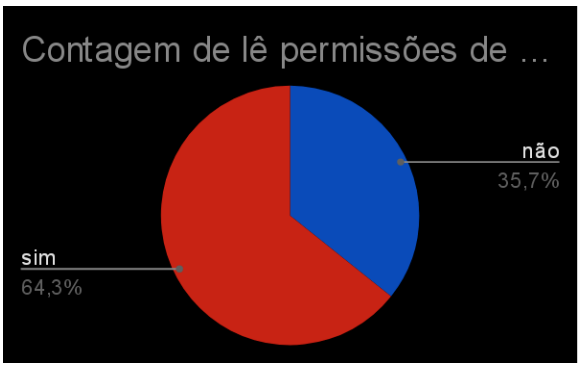
A etapa prática consistiu em uma pesquisa de campo do tipo levantamento (*survey*), realizada por meio da aplicação de um questionário digital estruturado, desenvolvido em uma aplicação web por um integrante do grupo, e respondido por estudantes da turma de Tecnologia em Sistemas para Internet (TSI 2026.1). O uso desse instrumento justifica-se por Marconi e Lakatos (2017), que destacam o questionário como uma técnica eficiente para a obtenção de dados padronizados, preservando o anonimato dos participantes. O instrumento combinou perguntas fechadas de caráter quantitativo, voltadas à análise de hábitos de segurança digital, e questões relacionadas à percepção de risco dos participantes. O questionário foi composto pelas seguintes perguntas:

1- Suas senhas geralmente tem mais de 8 caracteres?
2- Você verifica seus arquivos quando baixados?
3- Você evita usar redes Wi-Fi públicas para acessar contas importantes?
4- Você lê as permissões solicitadas por aplicativos antes de instalá-los?
5- Você evita compartilhar informações pessoais ou senhas com outras pessoas pela internet?
6- Você ativa a verificação em duas etapas quando disponível?
7- Você utiliza senhas diferentes para contas diferentes?
8- Você verifica se um site é confiável antes de inserir dados pessoais?

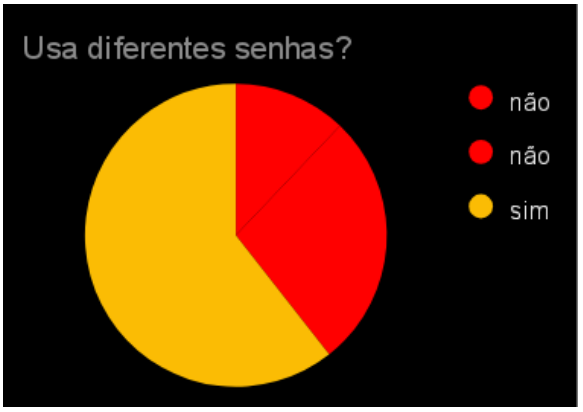
Visando os aspectos éticos, foi garantido o anonimato dos participantes por meio de Termo de Consentimento Livre e Esclarecido (TCLE), sem coleta de dados identificáveis. Os dados quantitativos foram analisados por meio de estatística descritiva.

RESULTADOS E DISCUSSÃO

Os resultados foram obtidos por meio de um questionário aplicado pelo grupo, com o objetivo de analisar os hábitos de segurança digital dos participantes, sendo estes por sua vez 32, no qual responderam nosso questionário.



Conforme apresentado no gráfico 1, 64,3% dos entrevistados afirmaram ler as permissões solicitadas pelos aplicativos antes de concedê-las, enquanto 35,7% declararam não possuir esse hábito. Esse resultado demonstra que parte dos usuários se preocupa com a privacidade de seus dados, porém uma parcela ainda concede permissões sem verificar as informações solicitadas. Essa prática aumenta os riscos de exposição de dados pessoais e compromete a segurança digital. De acordo com a Lei Geral de Proteção de Dados (LGPD) e a Cartilha de Segurança para Internet (CERT.br), verificar as permissões dos aplicativos é uma medida importante para proteger a privacidade e reduzir os riscos de uso indevido das informações.



Já o gráfico 2 mostra que 64,3% dos entrevistados utilizam senhas diferentes para cada serviço, enquanto 35,7% ainda utilizam a mesma senha em mais de uma conta. Embora a maioria adote uma prática considerada segura, o percentual de usuários que utilizam senhas ainda é preocupante, pois um único vazamento de credenciais pode comprometer diversas contas simultaneamente. O National Institute of Standards and Technology (NIST) recomenda a utilização de senhas únicas para cada serviço, enquanto a OWASP Foundation destaca a reutilização de senhas com uma das vulnerabilidades mais exploradas por criminosos virtuais.

Dessa forma, os resultados evidenciam que os participantes possuem certo nível de conscientização sobre segurança digital. Entretanto, ainda existem comportamentos que aumentam a vulnerabilidade dos usuários a ataques cibernéticos, reforçando a necessidade de ações educativas voltadas ao uso seguro da internet e à proteção de dados pessoais.

CONCLUSÃO

Com base no que foi apresentado, é possível concluir que os vazamentos de dados constituem uma das maiores ameaças à segurança digital nos dias de hoje, impactando diretamente a privacidade, a segurança e a qualidade de vida dos usuários. Os resultados do estudo mostram que esses incidentes podem levar a perdas financeiras, roubo de identidade, danos emocionais e divulgação não autorizada de dados pessoais. Além disso, constatou-se que ataques cibernéticos, erros humanos e vulnerabilidades nos sistemas desempenham um papel importante na ocorrência desses problemas. Conforme Galvão et al. (2024), a exposição indevida de informações pessoais representa um desafio crescente para a proteção da privacidade e para a garantia dos direitos dos cidadãos no ambiente digital. Nesse cenário, é essencial promover a conscientização dos usuários e adotar medidas de segurança digital, como senhas robustas, autenticação em dois fatores e atualização regular dos sistemas. Ademais, estudos apontam que os vazamentos de dados têm aumentado significativamente nos últimos anos, expondo bilhões de registros pessoais e reforçando a necessidade de mecanismos de proteção cada vez mais eficazes (MADNICK, 2023).

Por fim, com o progresso contínuo das tecnologias digitais, é essencial que usuários e instituições adotem práticas seguras no ambiente virtual. Aumentar a conscientização sobre os riscos e implementar medidas preventivas ajudam a reduzir incidentes e proteger a

AGRADECIMENTOS

Agradecemos ao professor orientador pelo apoio, orientação e pelos conhecimentos compartilhados durante o desenvolvimento deste trabalho. Também agradecemos à instituição por proporcionar os recursos necessários para a realização da pesquisa. Por fim, agradecemos aos nossos familiares e colegas pelo incentivo e apoio ao longo deste processo.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados: LGPD no cenário digital. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, n. 3, p. 26-45, jul./set. 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 26 jun. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 jun. 2026.

CERT.br. **Cartilha de Segurança para Internet**. São Paulo: NIC.br, 2026. Disponível em: https://cartilha.cert.br/. Acesso em: 27 jun. 2026.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010.

MADNICK, Stuart. *In*: APPLE. **Report**: 2.6 billion personal records compromised by data breaches in past two years — underscoring need for end-to-end encryption. Cupertino: Apple Newsroom, 2023. Disponível em: https://www.apple.com/br/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/. Acesso em: 27 jun. 2026.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 8. ed. São Paulo: Atlas, 2017.

OLIVEIRA, Larissa de Jesus; NOVAIS, Thyara Gonçalves. Lei Geral de Proteção de Dados Pessoais: responsabilidade civil no vazamento de informações. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 10, n. 5, p. 1614-1631, maio 2024. Disponível em: https://periodicorease.pro.br/rease/article/view/13668. Acesso em: 26 jun. 2026.

OWASP FOUNDATION. **Authentication**: OWASP Cheat Sheet Series. [S. l.]: OWASP, 2026. Disponível em: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html. Acesso em: 27 jun. 2026.

SCHUH, L. O. **Vulnerabilidade digital**: Estudo da percepção de segurança digital do jovem em Porto Alegre – RS. 2017. Trabalho de Conclusão de Curso (Graduação em Administração) – Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2017. Disponível em: https://lume.ufrgs.br/handle/10183/174693. Acesso em: 27 jun. 2026.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. e atual. Florianópolis: UFSC, 2005. Disponível em:

https://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf. Acesso em: 27 jun. 2026.