RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ANÁLISE DA RELAÇÃO ENTRE USABILIDADE E SEGURANÇA DA INFORMAÇÃO: UMA REVISÃO DE ESCOPO

ANALYSIS OF THE RELATIONSHIP BETWEEN USABILITY AND INFORMATION SECURITY: A SCOPING REVIEW

ANÁLISIS DE LA RELACIÓN ENTRE USABILIDAD Y SEGURIDAD DE LA INFORMACIÓN: UNA REVISIÓN DE ALCANCE

Larissa Júlia Ferreira Magalhães[1], Mária de Fátima Costa de Souza[2]

e636309
https://doi.org/10.47820/recima21.v6i3.6309

PUBLICADO: 3/2025

RESUMO

Usabilidade e segurança são frequentemente vistas como requisitos conflitantes no *design* de sistemas, especialmente para usuários não especializados. Este estudo apresenta uma revisão de escopo sobre a interseção entre usabilidade e segurança em sistemas digitais. Inicialmente, foram identificados 22.810 artigos, dos quais 19 atenderam aos critérios estabelecidos e foram analisados. Esses estudos investigaram desafios de usabilidade associados a vulnerabilidades de segurança, como autenticação complexa, dificuldades de navegação, interfaces sobrecarregadas e falta de clareza na comunicação de riscos. Além disso, foram avaliadas estratégias documentadas para mitigar esses problemas sem comprometer a proteção dos sistemas, incluindo *design* centrado no usuário, heurísticas de segurança, mecanismos de *feedback* adaptativo e interfaces multimodais. Os resultados indicam que problemas de usabilidade frequentemente contribuem para riscos de segurança, sendo a maioria dos estudos voltada para a identificação desses desafios em vez da validação de soluções. Estratégias como autenticação simplificada, técnicas de persuasão (*nudging*) e transparência na segurança demonstram potencial para equilibrar usabilidade e proteção, mas necessitam de maior validação empírica. Os achados apontam que a ausência de validação das soluções propostas em ambientes reais representa uma lacuna crítica na literatura, exigindo abordagens mais robustas para garantir sistemas simultaneamente seguros e utilizáveis. Pesquisas futuras devem se concentrar em avaliações quantitativas, testes práticos e adaptações baseadas em inteligência artificial para otimizar a segurança sem comprometer a experiência do usuário.

PALAVRAS-CHAVE: Usabilidade. Segurança da Informação. *Design* Centrado no Usuário.

ABSTRACT

Usability and security are often seen as conflicting requirements in system design, especially for non-specialized users. This study presents a scoping review on the intersection between usability and security in digital systems. Initially, 22.810 articles were identified, of which 19 met the established criteria and were analyzed. These studies investigated usability challenges associated with security vulnerabilities, such as complex authentication, navigation difficulties, overloaded interfaces, and lack of clarity in risk communication. Additionally, documented strategies to mitigate these problems without compromising system protection were evaluated, including user-centered design, security heuristics, adaptive feedback mechanisms, and multimodal interfaces. Results indicate that usability problems frequently contribute to security risks, with most studies focused on identifying these challenges rather than validating solutions. Strategies such as simplified authentication, persuasion techniques (nudging), and security transparency show potential for balancing usability and protection but require greater empirical validation. The findings highlight that the lack of validation of proposed solutions in real-world environments represents a critical gap in the literature, demanding more robust approaches to ensure systems that are both secure and usable. Future research should focus on quantitative assessments,

[1] Graduanda em Sistemas e Mídias Digitais pela Universidade Federal do Ceará.
[2] Doutora em Engenharia de Teleinformática pela Universidade Federal do Ceará e professora associada da Universidade Federal do Ceará.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

testing in real environments, and artificial intelligence-based adaptations to optimize security without compromising user experience.

KEYWORDS: *Usability. Information Security. User-Centered Design.*

RESUMEN
La usabilidad y la seguridad suelen considerarse requisitos conflictivos en el diseño de sistemas, especialmente para usuarios no especializados. Este estudio presenta una revisión de alcance sobre la intersección entre usabilidad y seguridad en los sistemas digitales. Inicialmente, se identificaron 22.810 artículos, de los cuales 19 cumplieron con los criterios establecidos y fueron analizados. Estos estudios investigaron los desafíos de usabilidad asociados con vulnerabilidades de seguridad, como autenticación compleja, dificultades de navegación, interfaces sobrecargadas y falta de claridad en la comunicación de riesgos. Además, se evaluaron estrategias documentadas para mitigar estos problemas sin comprometer la protección de los sistemas, incluyendo el diseño centrado en el usuario, heurísticas de seguridad, mecanismos de retroalimentación adaptativa e interfaces multimodales. Los resultados indican que los problemas de usabilidad contribuyen frecuentemente a riesgos de seguridad, y la mayoría de los estudios se centran en la identificación de estos desafíos en lugar de la validación de soluciones. Estrategias como autenticación simplificada, técnicas de persuasión (nudging) y transparencia en seguridad muestran potencial para equilibrar usabilidad y protección, pero requieren mayor validación empírica. Los hallazgos señalan que la falta de validación de las soluciones propuestas en entornos reales representa una brecha crítica en la literatura, exigiendo enfoques más sólidos para garantizar sistemas que sean simultáneamente seguros y utilizables. Las investigaciones futuras deben enfocarse en evaluaciones cuantitativas, pruebas en entornos reales y adaptaciones basadas en inteligencia artificial para optimizar la seguridad sin comprometer la experiencia del usuario.

PALABRAS CLAVE*: Usabilidad. Seguridad de la Información. Diseño Centrado en el Usuario.*

1. INTRODUÇÃO

No cenário digital atual, a relação entre usabilidade e segurança da informação tem se tornado cada vez mais crítica. À medida que os sistemas se tornam mais complexos e as ameaças cibernéticas mais sofisticadas, as organizações enfrentam o desafio de manter medidas de segurança robustas, garantindo que seus sistemas permaneçam acessíveis e fáceis de usar. Esse equilíbrio é particularmente crucial ao considerar usuários finais não especializados, que geralmente tomam decisões de segurança com base em sua compreensão dos elementos da interface (Sasse *et al.,* 2016).

Neste contexto, a usabilidade emerge como elemento fundamental, pois segundo a ISO 9241-11, ela representa a extensão em que um sistema, produto ou serviço pode ser usado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação em um contexto de uso específico (ISO 2020). A importância da usabilidade se reflete diretamente na interação dos usuários com recursos de segurança, uma vez que interfaces pouco intuitivas podem levá-los a contornar medidas de proteção, criando vulnerabilidades em sistemas que deveriam ser seguros (Whitten; Tygar 1999).

Por outro lado, a segurança da informação engloba a proteção contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação ou destruição de dados (NIST 2021). Embora seja fundamental implementar medidas de segurança, geralmente esta medida resulta em etapas adicionais

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ou complexidade nas interfaces do usuário, o que pode entrar em conflito com os princípios de usabilidade (Anderson, 2020).

Incidentes recentes destacam essa tensão e podem ser observados em estudos que demonstram que requisitos complexos de senha, geralmente, levam os usuários a criarem padrões previsíveis ou armazenar senhas de forma insegura (Florêncio; Herley; Van Oorschot, 2014). Da mesma forma, configurações de privacidade pouco claras em plataformas de mídia social já resultaram em divulgação não intencional de informações, demonstrando como o *design* da interface impacta diretamente os resultados de segurança (Bonneau; Preibusch, 2010).

Apesar do crescente reconhecimento desse problema, ainda persiste uma lacuna significativa na compreensão de como elementos específicos da interface afetam a segurança do sistema, especialmente quando se trata de usuários não especialistas. Esta questão ganhou ainda mais relevância recentemente, pois as ameaças cibernéticas têm se concentrado não apenas em vulnerabilidades técnicas, mas também em comportamentos humanos e suas interações com interfaces. Como resultado, somente em 2023, as perdas financeiras globais por violações de dados e ataques cibernéticos chegaram a ultrapassar US$ 8 trilhões, afetando tanto empresas quanto indivíduos (Gartner, 2023). Além disso, o mercado global de seguros cibernéticos obteve um crescimento expressivo nos últimos anos, conforme apresentado na Figura 1, impulsionado pelo aumento das ameaças digitais e ataques cibernéticos cada vez mais sofisticados. Este cenário pode ser comprovado com o relatório da GlobalData, que mostra que o setor passou de US$ 3,5 bilhões em 2016 para um valor estimado de US$ 33,4 bilhões em 2027. (Fraga, 2023).

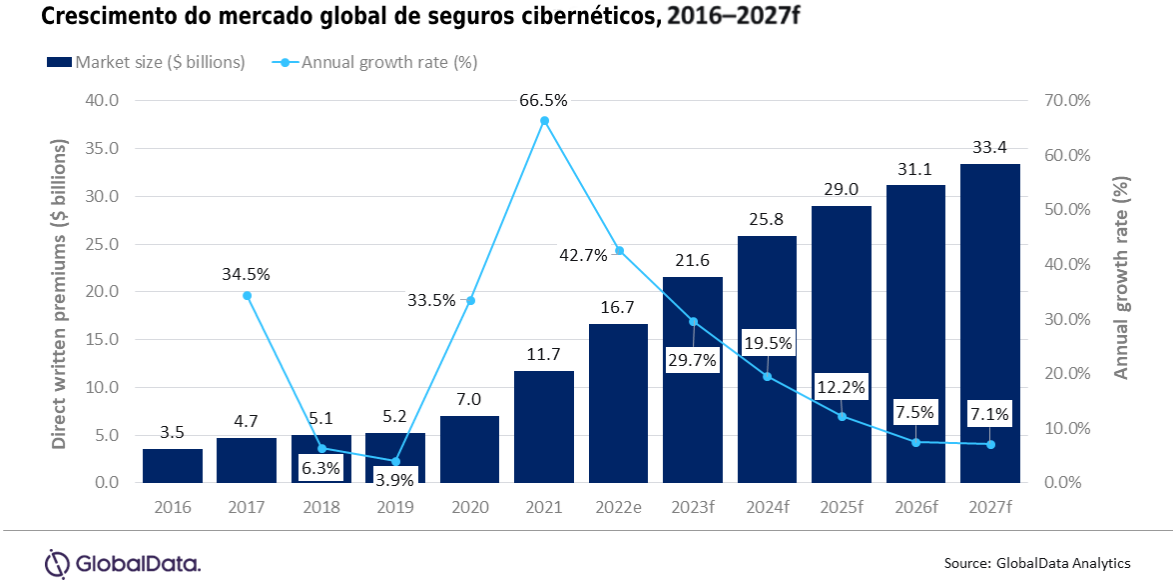

Figura 1 - Crescimento do mercado global de seguros cibernéticos. Fonte: (Fraga, 2023).

Diante desse cenário, o presente trabalho tem como objetivo realizar uma revisão de escopo no intuito de identificar elementos de interface que podem desencadear vulnerabilidades de segurança em sistemas voltados para usuários não especializados. Ao examinar pesquisas publicadas entre 2014

e 2024, o estudo traz análises sobre a relação entre decisões de usabilidade e resultados de segurança, com vista a contribuir para o desenvolvimento de sistemas simultaneamente seguros e utilizáveis.

2. MÉTODO

Considerando a natureza deste estudo, que visa investigar a relação entre usabilidade e segurança da informação em elementos de interface, foi conduzida uma revisão de escopo. Tal revisão, também conhecida como estudo de mapeamento sistemático, é um método amplamente utilizado para oferecer uma visão abrangente de uma área de pesquisa, com o objetivo de avaliar a disponibilidade, a abrangência e a qualidade das evidências existentes sobre um determinado tópico (Kitchenham; Charters, 2007).

Para a condução deste estudo, foram seguidas as diretrizes propostas por Dermeval *et al.,* (2020), que fornecem uma abordagem estruturada para garantir a reprodutibilidade e a confiabilidade do processo. Adicionalmente às diretrizes mencionadas, foi utilizada a ferramenta de gerenciamento Parsif.al para auxiliar no planejamento, execução e documentação da revisão. O processo também seguiu as etapas recomendadas por Arksey e O'Malley (2005) e ampliadas por Levac *et al.,* (2010), incluindo:

1. Identificação clara dos objetivos e questões de pesquisa (RQs).
2. Seleção criteriosa das fontes de dados e estratégias de busca.
3. Extração e análise dos dados relevantes.
4. Resumo e apresentação dos resultados em formato estruturado.

No início do processo, foram definidas as questões de pesquisa (RQs) que guiaram a revisão. Essas questões foram elaboradas para abordar os principais aspectos do tema e garantir que o estudo mapeasse as lacunas e as tendências existentes. Um total de duas questões de pesquisa (RQs) foram formuladas, nas quais cada uma delas foi alinhada aos objetivos do estudo e descrita como:

QP1. Quais são os elementos de usabilidade mais frequentemente associados a vulnerabilidades de segurança em sistemas projetados para usuários finais não especializados?

QP2. Quais são as estratégias adotadas e bem-sucedidas documentadas na literatura para equilibrar requisitos de usabilidade e segurança da informação em sistemas voltados para usuários não especialistas?

2.1. Busca e seleção de estudos

As fontes primárias utilizadas para coleta dos estudos a serem analisados foram Scopus e Google Scholar, tendo como critério de escolha a acessibilidade por meio de credenciais institucionais acadêmicas e a disponibilidade gratuita do conteúdo. Para garantir um levantamento abrangente da literatura, foi empregada um[1]a abordagem de busca em duas etapas. Na primeira etapa, utilizou-se a

[1] https://parsif.al/

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

string de busca inicial: *"usability AND ("information security" OR cybersecurity) AND ("user interface" OR interface)"*. Posteriormente, para ampliar o alcance e identificar estudos adicionais, foram incorporados sinônimos e termos relacionados na segunda etapa de busca: *"(usability OR user experience OR UX) AND (information security OR cybersecurity OR data protection) AND (interface design OR UI elements OR interaction design)"*.

Para garantir a relevância e a qualidade dos estudos incluídos no mapeamento, foi estabelecido um conjunto de critérios de inclusão e exclusão, conforme apresentado na Tabela 1. Nos critérios de inclusão, foram considerados artigos científicos publicados entre 2014 e 2024, disponíveis nos idiomas português e/ou inglês, que abordassem diretamente a relação entre usabilidade e segurança da informação e que fossem focados em usuários finais não especializados. Para os critérios de exclusão, foram descartadas publicações que não fossem artigos científicos originais, estudos sem acesso ao texto completo e pesquisas que não contemplam especificamente a relação entre usabilidade e sistemas de segurança. Esses critérios foram projetados para filtrar os resultados da pesquisa e selecionar apenas os estudos que pertencessem diretamente aos objetivos e tema desta pesquisa. Os critérios, detalhados, de inclusão e exclusão são apresentados na Tabela 1.

Critérios de inclusão	Critérios de exclusão
Artigos científicos publicados entre 2014 e 2024	Artigos científicos não originais
Disponíveis nos idiomas português e/ou inglês	Estudos sem acesso ao texto completo
Aborda diretamente a relação entre usabilidade e segurança da informação e são focados em usuários finais não especializados	Pesquisas que não contemplam especificamente a relação entre usabilidade de interface e sistemas de segurança

Tabela 1 - Critérios de inclusão e exclusão

No total, foram identificados, nas duas etapas de busca, 22.810 estudos. Após a remoção automática de duplicatas utilizando o Parsif.al[1], restaram 11.116 artigos. Em seguida, foi realizada uma triagem inicial baseada na análise de títulos, data de publicação, palavras-chave e resumos, seguindo os critérios de exclusão, o que resultou na retirada de 10.955 estudos, restando 161 artigos. Na etapa final, os artigos foram avaliados integralmente, e aqueles que não atendiam aos critérios de inclusão foram removidos, culminando na seleção de 19 estudos finais para análise. O processo de seleção foi conduzido por um único pesquisador, responsável por aplicar os critérios de inclusão e exclusão de forma sistemática. O processo de seleção detalhado é ilustrado na Figura 2. Esse procedimento resultou na seleção final de 19 estudos elegíveis para inclusão na revisão sistemática. A lista final de estudos e suas abreviações é fornecida na Tabela 3.

Embora o processo de triagem tenha sido conduzido de forma sistemática e seguindo critérios predefinidos, é importante reconhecer que a ausência de uma avaliação independente por parte de um segundo pesquisador pode representar uma limitação em termos de replicabilidade do processo. A

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

falta de um segundo avaliador pode introduzir vieses inconscientes na seleção dos artigos, especialmente na interpretação dos critérios de inclusão e exclusão.

Os parágrafos a seguir apresentam as análises feitas em cima desses artigos a fim de responder às questões de pesquisa.

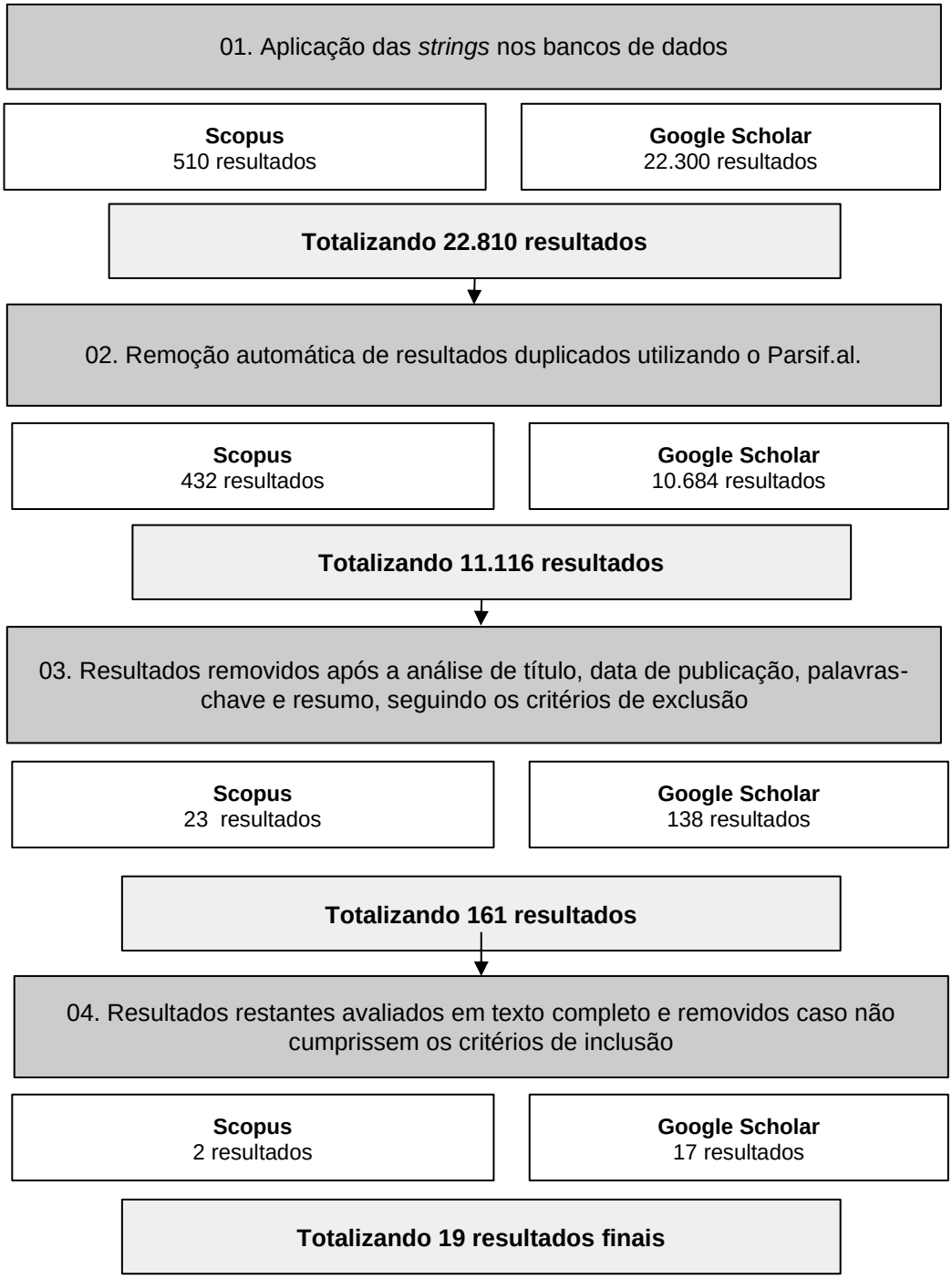

Figura 2. Processo de seleção detalhado

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

2.2. Análise de dados

Para conduzir a análise de dados, foram formuladas perguntas específicas para cada questão de pesquisa, formando um formulário de extração de dados descrito na Tabela 2. Durante a revisão dos artigos, foi realizada uma leitura exploratória e extração dos dados de acordo com o formulário.

#	Dados do Estudo
1	Autores, ano, título
2	Fonte do estudo (periódico, conferência, etc.)
3	Metodologia de pesquisa (pesquisa, experimento, estudo de caso, etc.)
4	Quantos participantes estavam envolvidos?
5	Quem eram os participantes (por exemplo, usuários finais, profissionais de TI, público em geral)?
6	Qual era o objetivo principal do estudo?
7	Qual sistema, funcionalidade ou aplicativo foi avaliado?
8	Quais elementos de usabilidade foram analisados no estudo?
9	Algum problema de usabilidade estava vinculado a vulnerabilidades de segurança? Se sim, quais?
10	Quais foram os problemas de usabilidade mais frequentemente mencionados em relação à segurança?
11	Como os problemas de usabilidade impactaram os riscos de segurança?
12	Houve alguma violação ou incidente de segurança relatado devido a falhas de usabilidade?
13	Houve recomendações para melhorar a usabilidade sem comprometer a segurança?
14	Quais estratégias foram usadas para equilibrar usabilidade e segurança no sistema?
15	As estratégias foram testadas ou validadas em cenários do mundo real?
16	As estratégias levaram a melhorias mensuráveis em usabilidade e/ou segurança?
17	Houve alguma compensação mencionada entre usabilidade e segurança?
18	Quais foram os desafios encontrados na implementação dessas estratégias?
19	Houve algum benefício ou desvantagem adicional relatado?

Tabela 2 - Formulário de extração de dados

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Nº	Título	Autor (Ano)
S1	*A Human-Centered Design Methodology to Enhance the Usability, Human Factors, and User Experience of Connected Health Systems*	Richard Harte et al. (2017)
S2	*A cloud-edge based data security architecture for sharing and analysing cyber threat information*	David W Chadwick, Wenjun Fan, Gianpiero Costantino, Rogerio de Lemos, Francesco Di Cerbo, Ian Herwono, Mirko Manea, Paolo Mori, Ali Sajjad, Xiao-Si Wang (2020)
S3	*Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos*	Yifang Li, Nishant Vishwamitra, Bart P. Knijnenburg, Hongxin Hu, Kelly Caine (2017)
S4	*Usable Cybersecurity: a Contradiction in Terms?*	Steven Furnell (2024)
S5	*Designing a Secure Interactive System: Balancing the Conflict Between Security, Usability, and Functionality*	Esther Oluwatobi Akinlade, Elizabeth Omolara Adeleye (2022)
S6	*Toward a Knowledge Graph of Cybersecurity Countermeasures*	Peter E. Kaloroumakis, Michael J. Smith (2021)
S7	*Leveraging human factors in cybersecurity: an integrated methodological approach*	Alessandro Pollini, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, Davide Guerri (2022)
S8	*Privacy-Friendly Nudging Strategies for Security and Privacy Decisions*	Schneider, W., Fischer-Hübner, S. (2018)
S9	*Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios*	Martin Schrepp, Andreas Hinderks, Jörg Thomaschewski (2014)
S10	*Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control*	W. Kasprzak, W. Szynkiewicz, M. Stefańczyk, W. Dudek, M. Węgierek, D. Seredyński, M. Figat, C. Zieliński (2020)
S11	*Development of the Software Application with Graphical User Interface for One Model Cyber Security*	Ramaz R. Shamugia (2019)
S12	*A Client-Centered Information Security and Cybersecurity Auditing Framework*	Mário Antunes, Marisa Maximiano, Ricardo Gomes (2022)
S13	*Usability Issues of Virtual Reality Learning Simulator in Healthcare and Cybersecurity*	Jussi Kasurinen (2017)
S14	*Concept of Using Eye Tracking Technology to Assess and Ensure Cybersecurity, Functional Safety and Usability*	Oleksandr Gordieiev, Vyacheslav Kharchenko, Oleg Illiashenko, Olga Morozova, Magomediemin Gasanov (2021)
S15	*Usability of Safety Critical Applications in Enterprise Environments*	Gabriele Sambin (2023)
S16	*Cybersecurity for the Unbanked: Usable Security Heuristics for Mobile Financial Services*	Stephen Mathew Ambore (2024)

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Nº	Título	Autor (Ano)
S17	*Usable Security Versus Secure Usability: an Assessment of Attributes*	Oleksandr Gordieiev, Vyacheslav Kharchenko, Kate Vereshchak (2024)
S18	*Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula*	Shana Kayne Beach (2014)
S19	*Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study*	Santiago Criollo-C, Andrea Guerrero-Arias, Diego Buenaño-Fernández, Sergio Luján-Mora (2024)

Tabela 3 - Estudos incluídos

Para responder à QP1— Quais são os elementos de usabilidade mais frequentemente associados a vulnerabilidades de segurança em sistemas projetados para usuários finais não especializados? — Foram analisados os estudos selecionados que discutem a relação entre usabilidade e segurança. A extração de informações focou em identificar problemas de usabilidade mencionados, como complexidade na autenticação, dificuldade de navegação, interfaces sobrecarregadas e falta de transparência na comunicação sobre riscos de segurança. Também foram consideradas as categorias de usuários afetados e os sistemas em que essas vulnerabilidades foram mais frequentemente observadas.

Para responder à QP2 — Quais são as estratégias bem-sucedidas documentadas na literatura para equilibrar requisitos de usabilidade e segurança da informação em sistemas voltados para usuários não especialistas? — foram avaliadas as recomendações dos estudos para mitigar os impactos negativos da usabilidade na segurança. A revisão incluiu a análise de estratégias como *design* centrado no usuário, implementação de heurísticas específicas para segurança utilizável, redução da carga cognitiva das interfaces e aprimoramento do *feedback* ao usuário. Também foram verificadas evidências quantitativas e qualitativas sobre a eficácia dessas estratégias, incluindo testes de usabilidade, validações em cenários reais e impacto percebido pelos participantes dos estudos.

3. RESULTADOS E DISCUSSÕES

Dos 19 artigos selecionados, 15 abordam a experiência do usuário e usabilidade de sistemas de segurança cibernética, enquanto 6 focam na interação entre segurança e fatores humanos. A perspectiva de segurança utilizável tem sido um tema recorrente, mas há uma necessidade de explorar mais profundamente a interseção entre usabilidade e segurança em contextos críticos.

A distribuição geográfica dos estudos revela que as pesquisas foram realizadas em diferentes locais, incluindo Estados Unidos, Reino Unido, Noruega, Alemanha, Turquia, China, Itália, Portugal, Brasil e Polônia. Essa diversidade sugere um interesse global na investigação sobre segurança e usabilidade. Entre os artigos, os Estados Unidos aparecem mais frequentemente, seguidos por estudos realizados na Europa.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Em relação ao nível de aplicação, os estudos analisaram diferentes contextos de uso da segurança cibernética. 14 estudos focaram em aplicações para o público geral e usuários finais, enquanto 7 abordaram ambientes especializados, como saúde, educação e infraestrutura crítica. A predominância do público geral denota um interesse maior na acessibilidade de soluções de segurança para usuários comuns, embora haja uma lacuna na investigação da aplicabilidade em setores específicos.

Nos estudos analisados, foram identificadas diversas vulnerabilidades de segurança relacionadas à usabilidade. Um dos principais problemas mencionados é a complexidade excessiva nos processos de autenticação, o que muitas vezes leva os usuários a tentarem contornar as medidas de segurança para facilitar o acesso. Além disso, a baixa acessibilidade e as dificuldades na navegação comprometem a adoção de práticas seguras, tornando o uso dos sistemas menos intuitivo. Outro aspecto crítico é a sobrecarga de informações nas interfaces, o que pode gerar riscos operacionais e aumentar a chance de erros na tomada de decisão. A falta de transparência na comunicação sobre riscos de segurança também foi apontada como um fator preocupante, pois pode resultar na exposição involuntária de dados sensíveis.

Para mitigar essas vulnerabilidades sem comprometer a segurança, os estudos sugerem algumas estratégias. A primeira delas é a adoção de um *design* centrado no usuário, priorizando a clareza e a acessibilidade das interfaces. Também se recomenda o uso de heurísticas específicas para segurança utilizável, garantindo um equilíbrio entre proteção e experiência do usuário. Além disso, a redução da carga cognitiva das interfaces pode simplificar os processos sem diminuir a eficácia das medidas de segurança. Outra proposta importante é a implementação de *feedback* contínuo ao usuário, permitindo que ele compreenda melhor os riscos envolvidos e tome decisões mais informadas.

A análise dos artigos evidencia um padrão recorrente: há um *trade-off* entre segurança e usabilidade. Muitas vezes, medidas mais rigorosas de proteção resultam em barreiras adicionais para os usuários, tornando o sistema mais difícil de utilizar. No entanto, os estudos também indicam que estratégias bem projetadas podem minimizar esse impacto, garantindo que os sistemas de segurança sejam não apenas eficazes, mas também acessíveis e intuitivos.

3.1. Objetivo

Nas pesquisas, os objetivos de uso foram analisados nos 19 estudos revisados e classificados conforme suas finalidades. Inicialmente, foram definidas duas categorias gerais: "Usabilidade e Segurança", para os 17 estudos (80,95%) que analisam como a experiência do usuário impacta a segurança cibernética, e "Estratégias de Mitigação", para os 4 estudos (19,05%) que exploram soluções para melhorar a segurança sem comprometer a usabilidade.

Dentro da categoria "Usabilidade e Segurança", foram identificadas três subcategorias específicas. A subcategoria "Problemas de Usabilidade" foi abordada em 8 estudos (42,11%), analisando falhas na experiência do usuário relacionadas a vulnerabilidades de segurança. A

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

subcategoria "Impacto na Segurança" foi tratada em 6 estudos (31,58%), que demonstram como problemas de usabilidade podem levar a riscos de segurança. Por fim, a subcategoria "Casos Específicos" inclui 3 estudos (15,79%), englobando análises de situações reais ou estudos de caso de sistemas e aplicativos.

Na categoria "Estratégias de Mitigação", os 2 estudos (10,53%) foram agrupados de forma geral, pois a maioria apresenta recomendações e boas práticas sem uma separação rigorosa de estratégias. Os principais enfoques incluem o uso de *design* centrado no usuário, heurísticas de segurança utilizável, adaptação da interface e aprimoramento de *feedbacks* para usuários.

A classificação dos 19 estudos com base nesses objetivos ajuda a estruturar um mapeamento das pesquisas na área. Cada estudo pode se encaixar em mais de uma subcategoria, mas observamos que não há estudos que pertençam simultaneamente às duas categorias gerais. Em termos de quantidade, a maioria dos estudos está concentrada na categoria "Usabilidade e Segurança", indicando um interesse predominante em identificar problemas antes de propor soluções. A distribuição específica, considerando as subcategorias, está detalhada na Tabela 4.

Objetivo Principal	Subcategoria	Estudos	Frequência (%)
Usabilidade e Segurança	Problemas de Usabilidade	S01, S03, S05, S07, S09, S10, S12 , S14.	8 (42,11%)
	Impacto na Segurança	S02, S06, S08, S11, S13, S15.	6 (31,58%)
	Casos Específicos	S04, S16, S17.	3 (15,79%)
Estratégias de Mitigação	N/A	S18 e S19.	2 (10,53%)

Tabela 4 - Estudos sobre objetivo primário

QP1. Quais são os elementos de usabilidade mais frequentemente associados a vulnerabilidades de segurança em sistemas projetados para usuários finais não especializados?

Para identificar os elementos de usabilidade que mais impactam a segurança, analisamos os estudos disponíveis e categorizamos os problemas relatados. Os resultados mostram que diferentes aspectos da interface e da interação dos usuários podem levar a vulnerabilidades, seja por dificuldades de uso ou por incentivos inadequados às práticas inseguras.

A autenticação complexa foi o elemento mais citado, aparecendo em 6 estudos. Os relatos indicam que mecanismos de autenticação muito rígidos ou difíceis de compreender incentivam os usuários a reutilizarem senhas fracas, anotar credenciais em locais inseguros ou até desativar recursos de segurança sempre que possível. Isso compromete a integridade dos sistemas e pode facilitar ataques como *phishing* e roubo de credenciais.

A presença de interfaces pouco intuitivas foi apontada em 5 estudos, destacando que dificuldades na navegação e na compreensão das funcionalidades dos sistemas levam os usuários a adotarem comportamentos inseguros, como ignorar alertas de segurança ou utilizar atalhos que

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

reduzem a proteção. Interfaces mal projetadas reduzem a percepção de risco dos usuários, tornando-os mais vulneráveis a ameaças digitais.

Outro problema relevante foi o excesso de informações, mencionado em 4 estudos. Sistemas que apresentam muitas opções, notificações ou textos extensos acabam sobrecarregando o usuário cognitivamente, fazendo com que decisões importantes sejam tomadas de forma apressada ou negligente. Como resultado, usuários podem ignorar configurações de privacidade, conceder permissões excessivas a aplicativos ou não perceber riscos de segurança embutidos em determinadas funcionalidades.

A falta de clareza na comunicação de riscos foi evidenciada em 4 estudos, demonstrando que mensagens pouco claras ou alarmistas podem levar à tomada de decisões equivocadas. Muitos sistemas apresentam alertas genéricos ou ambíguos que não explicam de forma objetiva as consequências de uma ação específica, o que pode resultar em permissões concedidas indevidamente ou em falhas na configuração de segurança.

A baixa acessibilidade também foi relatada como um fator crítico em 3 estudos. Interfaces que não levam em consideração usuários com necessidades especiais, dificuldades motoras ou limitações visuais acabam restringindo o uso seguro do sistema para um público significativo. Como consequência, esses usuários podem adotar alternativas menos seguras para contornar dificuldades de acesso.

Enquanto a dificuldade na navegação segura foi apontada em 3 estudos, destacando que a falta de um fluxo lógico na interface pode fazer com que usuários desconsiderem opções seguras ou não saibam como ativá-las. Sistemas que exigem múltiplas etapas para configuração de segurança tendem a ter baixa adesão às boas práticas, resultando em vulnerabilidades exploráveis.

A análise mostra que os problemas de usabilidade impactam diretamente a segurança dos sistemas, muitas vezes levando usuários a adotarem práticas arriscadas ou a desativarem mecanismos de proteção. A literatura sugere que melhorias na interface e na interação dos usuários podem reduzir significativamente essas vulnerabilidades sem comprometer a eficácia dos sistemas de segurança.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

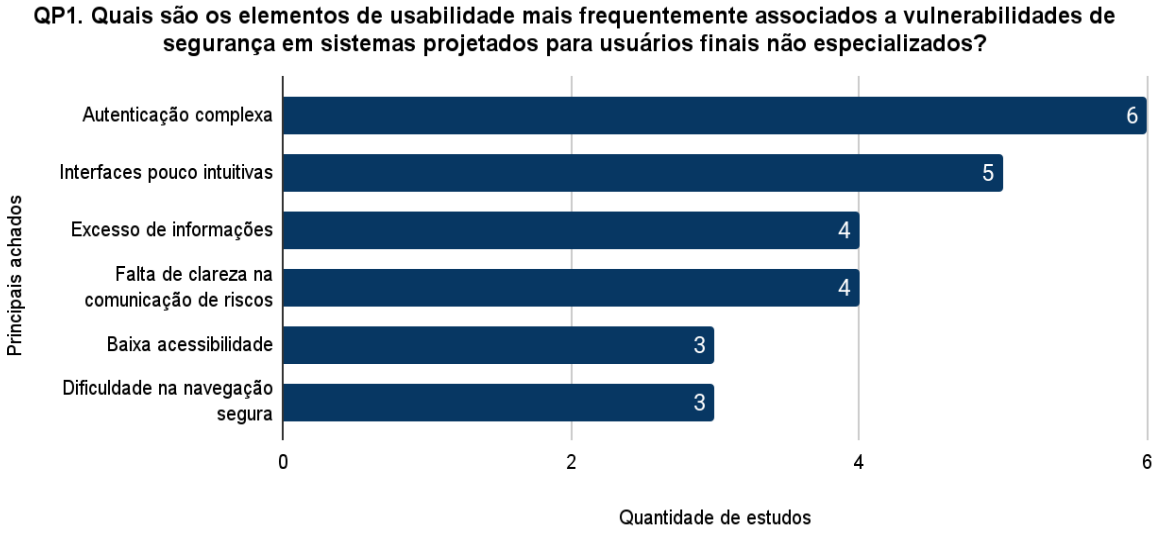

Figura 3 - Principais achados da 1° Questão de Pesquisa (QP1)

QP2. Quais são as estratégias bem-sucedidas documentadas na literatura para equilibrar requisitos de usabilidade e segurança da informação em sistemas voltados para usuários não especialistas?

Para responder a essa questão, foram analisados os estudos que exploram estratégias aplicadas ao equilíbrio entre usabilidade e segurança. As abordagens identificadas foram agrupadas em diferentes categorias de soluções.

Em relação ao *design* centrado no usuário, 6 estudos destacaram a importância de interfaces acessíveis e intuitivas para garantir que usuários sem conhecimento técnico consigam interagir com sistemas seguros de forma eficiente. As principais recomendações envolvem simplificação de processos, maior transparência na comunicação de riscos e personalização da interface para diferentes perfis de usuários.

A adoção de heurísticas de segurança utilizável foi documentada em 4 estudos, propondo diretrizes específicas para equilibrar proteção e experiência do usuário. Estratégias como autenticação simplificada, *feedback* claro sobre riscos e controle granular de acessos foram destacadas como métodos eficazes para manter a segurança sem comprometer a usabilidade.

Os mecanismos de persuasão para segurança e privacidade (*nudging*) apareceram em 3 estudos, sugerindo abordagens como notificações adaptativas, avisos contextuais e recomendações personalizadas para incentivar boas práticas de segurança sem sobrecarregar o usuário. Os resultados indicam que essas técnicas podem aumentar a adoção de medidas seguras sem impactar negativamente a experiência do usuário.

Outro enfoque relevante foi o uso de interfaces multimodais, documentado em 3 estudos, que exploram a integração de comandos de voz, gestos e elementos visuais para melhorar a interação com

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

sistemas de segurança. Essa abordagem demonstrou potencial para aumentar a eficiência dos usuários na detecção e resposta a ameaças.

A implementação de modelos de confiança e níveis de acesso foi mencionada em 2 estudos, que propõem diferentes camadas de proteção e anonimização de dados para otimizar a colaboração entre usuários sem comprometer a segurança da informação.

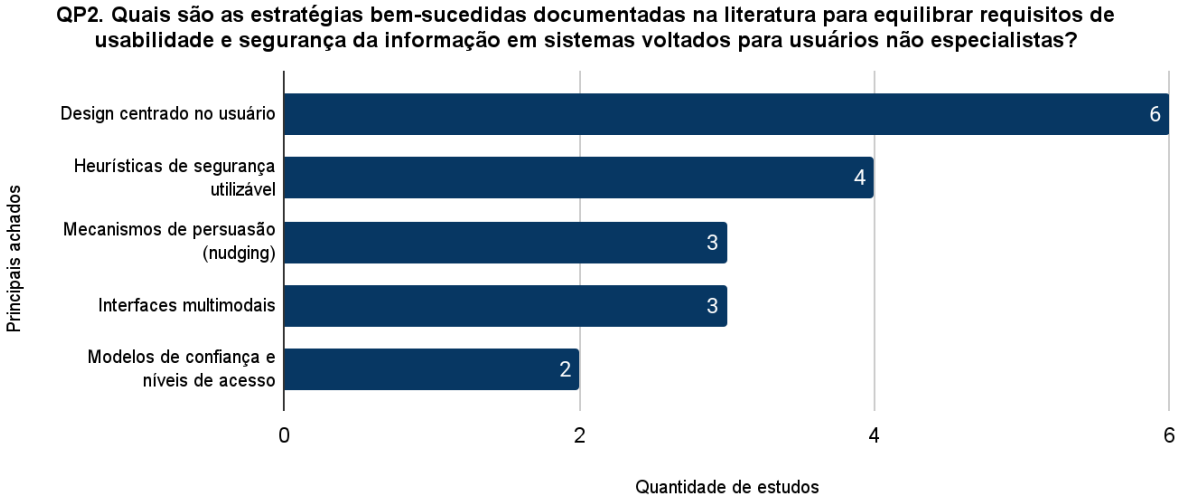

Figura 4 - Principais achados da 2° Questão de Pesquisa (QP2)

De forma geral, a literatura sugere que o equilíbrio entre usabilidade e segurança pode ser alcançado por meio de abordagens iterativas e testes contínuos com usuários finais. No entanto, a maioria dos estudos analisados destaca a necessidade de mais pesquisas quantitativas para validar o impacto dessas estratégias em ambientes reais, onde fatores como diversidade de usuários, complexidade organizacional e restrições de recursos podem impactar significativamente a eficácia dessas estratégias.

Muitas das soluções propostas, como autenticação simplificada e *feedback* adaptativo, dependem de adaptações contextuais que variam conforme o público-alvo e a natureza dos sistemas de segurança. O que pode ser eficaz para um usuário comum pode não ser adequado para sistemas críticos, como os utilizados em infraestruturas governamentais ou ambientes corporativos de alta segurança.

Portanto, embora as estratégias propostas sejam teoricamente sólidas, sua aplicação em contextos reais requer uma abordagem mais pragmática, considerando as limitações e desafios específicos de cada ambiente.

4. CONCLUSÃO E TRABALHOS FUTUROS

Este estudo realizou um mapeamento sistemático da literatura sobre a relação entre usabilidade e segurança da informação em sistemas voltados para usuários não especializados. No total, foram identificados 22.810 artigos nas bases de dados consultadas. Após a remoção de duplicatas e a aplicação dos critérios de exclusão, 161 estudos foram selecionados para avaliação em

texto completo. Desses, 19 atenderam aos critérios estabelecidos e foram analisados. A análise desses estudos revelou que problemas de usabilidade, como autenticação complexa, dificuldades de navegação, interfaces sobrecarregadas e falta de clareza na comunicação de riscos, estão frequentemente associados a vulnerabilidades de segurança. Além disso, os resultados mostram que estratégias como o *design* centrado no usuário, heurísticas de segurança utilizável, mecanismos de persuasão *(nudging)* e interfaces multimodais podem mitigar esses problemas sem comprometer a proteção dos sistemas. No entanto, a maioria dos estudos carece de avaliações quantitativas sobre a eficácia dessas estratégias, indicando que a principal limitação identificada nesta revisão diz respeito à ausência de validação empírica robusta dos métodos propostos.

Apesar dos avanços documentados, ainda há desafios significativos, incluindo a dificuldade de implementação de medidas de segurança sem impactar a experiência do usuário, a resistência organizacional a mudanças e a falta de conscientização dos usuários sobre os riscos de segurança. Diante desses achados, tem-se como proposta para trabalhos futuros investigar a validação empírica das estratégias propostas, a exploração de novas abordagens baseadas em inteligência artificial e aprendizado adaptativo, e a realização de estudos que investiguem a percepção dos usuários sobre segurança digital. Além disso, o aumento de colaborações entre pesquisadores e desenvolvedores de *software* também se mostra essencial para integrar princípios de *design* centrado no usuário e segurança desde a concepção dos sistemas.

Com isso, essas pesquisas podem contribuir para o desenvolvimento de sistemas mais seguros, acessíveis e intuitivos, garantindo que a segurança seja incorporada de maneira eficiente e transparente para usuários não especializados.

REFERÊNCIAS

AKINLADE, E. O.; ADELEYE, E. O. **Designing a Secure Interactive System:** Balancing the Conflict Between Security, Usability, and Functionality. [*S. l.: s. n.*], 2022.

AMBRORE, S. M. **Cybersecurity for the Unbanked:** Usable Security Heuristics for Mobile Financial Services. 2024. Thesis - Bournemouth University, 2024.

ANDERSON, B. R.; JOHNSON, J. T. Securing Vehicle Charging Infrastructure Against Cybersecurity Threats. *In*: **Conference** [...] SAE Hybrid and Electric Vehicle Symposium, 2020. Disponível em: https://doi.org/10.13140/RG.2.2.28243.12329. Acesso em: 07 fev. 2025.

ANDERSON, R. **Security Engineering:** A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020. Disponível em: https://github.com/tpn/pdfs/blob/master/Security%20Engineering%20%20Ross%20Anderson%20(v1).pdf. Acesso em: 12 fev. 2025.

ANTUNES, M.; MAXIMIANO, M.; GOMES, R. A Client-Centered Information Security and Cybersecurity Auditing Framework. **Applied Sciences**, v. 12, 2022. Disponível em: https://doi.org/10.3390/app12094102. Acesso em: 07 fev. 2025.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ARKSEY, H.; O'MALLEY, L. Scoping studies: towards a methodological framework. **International Journal of Social Research Methodology,** v. 8, n. 1, p. 19-32, 2005. Disponível em: https://doi.org/10.1080/1364557032000119616. Acesso em: 07 fev. 2025.

BEACH, S. K. Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula. **National Cybersecurity Institute Journal,** v. 1, n. 1, 2014.

BONNEAU, J.; PREIBUSCH, S. **The Privacy Jungle:** On the Market for Data Protection in Social Networks. [*S. l.: s. n.*], 2010. Disponível em: https://doi.org/10.1007/978-1-4419-6967-58. Acesso em: 12 fev. 2025.

CHADWICK, D. W. *et al.* A cloud-edge based data security architecture for sharing and analysing cyber threat information. **Future Generation Computer Systems**, v. 102, 2020.

CRIOLO-C, S. et al. Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study. **IEEE Access**, 2024.

DERMEVAL, D.; COELHO, J.; BITTENCOURT, I. I. Mapeamento Sistemático e Revisão Sistemática da Literatura em Informática na Educação. *In:* **Metodologia de Pesquisa Científica em Informática na Educação**: Abordagem Quantitativa. Porto Alegre: SBC, 2020. p. 26. v. 2.

FLORÊNCIO, D.; HERLEY, C.; VAN OORSCHOT, P. C. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. *In:* **USENIX Conference on Security Symposium**, San Diego, 20-22 ago. 2014, p. 575-590.

FRAGA, N. Aumento de ataques cibernéticos reforça a importância do seguro cyber. **Revista Apólice**, 2023. Disponível em: https://revistaapolice.com.br/2023/07/aumento-de-ataques-ciberneticos-reforca-a-importancia-do-seguro-cyber/. Acesso em: 12 out. 2024.

FURNELL, S. **Usable Cybersecurity:** a Contradiction in Terms? [*S. l.: s. n.*]. 2024.

GARTNER. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024. **Gartner Press Releases**, 2023. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecastsglobalsecurity-and-risk-management-spending-to-grow-14-percent-in-2024. Acesso em: 10 out. 2024.

GORDIEIEV, O. *et al.* Concept of Using Eye Tracking Technology to Assess and Ensure Cybersecurity, Functional Safety and Usability. **International Journal of Safety and Security Engineering**, v. 11, n. 4, 2021.

GORDIEIEV, O.; KHARCHENKO, V.; VERESHCHAK, K. **Usable Security Versus Secure Usability:** an Assessment of Attributes Interaction. [S. l.]: Banking University, National Aerospace University «KhAI», Luxoft, 2024.

HARTE, R. *et al.* A Human-Centered Design Methodology to Enhance the Usability, Human Factors, and User Experience of Connected Health Systems. **JMIR Human Factors**, v. 4, n. 1, 2017.

ISO. **ISO 9241-110:** Ergonomics of Human-System Interaction-Pt. 110: Interaction Principles. [S. l.]: ISO, 2020.

KALOROUMAKIS, P. E.; SMITH, M. J. **Toward a Knowledge Graph of Cybersecurity Countermeasures.** [S. l.]: MITRE Corporation, 2021.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

KASPRZAK, W. *et al.* Agent-based approach to the design of a multimodal interface for cyber-security event visualisation control. **Bulletin of the Polish Academy of Sciences: Technical Sciences**, v. 68, n. 5, 2020.

KASURINEN, J. Usability Issues of Virtual Reality Learning Simulator in Healthcare and Cybersecurity. **Procedia Computer Science**, v. 119, 2017.

KITCHENHAM, B.; CHARTERS, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering.** EBSE Technical Report EBSE-2007-01. **School of Computer Science and Mathematics**, Keele, UK, 2007.

LEVAC, D.; COLQUHOUN, H.; O'BRIEN, K. K. Scoping studies: advancing the methodology. **Implementation Science**, v. 5, n. 1, p. 69, 2010. Disponível em: http://doi.org/10.1186/1748-5908-5-69. Acesso em: 07 fev. 2025.

LI, Y. *et al.* Effectiveness and Users' Experience of Obfuscation as a Privacy-Enhancing Technology for Sharing Photos. **Proceedings of the ACM on Human-Computer Interaction**, v. 1 (CSCW), 2017.

NIST. National Institute of Standards and Technology. **Cybersecurity Framework (CSF)**., abr. 2018. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 12 fev. 2025.

POLLINI, A. *et al.* Leveraging human factors in cybersecurity: an integrated methodological approach. **Cognition, Technology & Work**, 2022.

SAMBIN, G. **Usability of Safety Critical Applications in Enterprise Environments. 2023.** Master (Degree Course in Computer Engineering) - Politecnico di Torino, 2023.

SASSE, A.; SMITH, M. The Security-Usability Tradeoff Myth. **IEEE Security & Privacy**, v. 14, p. 11-13, 2016. Disponível em: https://doi.org/10.1109/MSP.2016.102. Acesso em: 07 fev. 2025.

SCHNEIDER, W.; FISCHER-HÜBNER, S. **Privacy-Friendly Nudging Strategies for Security and Privacy Decisions.** Privacy and Identity Management. The Fairness Challenge (Springer), 2018.

SCHREPP, M.; HINDERKS, A.; THOMASCHEWSKI, J. Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. **Lecture Notes in Computer Science (LNCS),** 2014.

SHAMUGIA, R. R. Development of the Software Application with Graphical User Interface for One Model Cyber Security. **International Journal of Communications, Network and System Sciences**, v. 12, 2019. Disponível em: https://doi.org/10.4236/ijcns.2019.1212014. Acesso em: 07 fev. 2025.

WHITTEN, A.; TYGAR, J. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. **Proceedings of the 8th USENIX Security Symposium**, v. 8, p. 14, 1999.