



O Uso de Jogos Sérios para o Ensino de Higiene Cibernética: Uma Revisão Sistemática

Nicolas Chagas Souza, UnB, nszchagas@gmail.com,
<https://orcid.org/0009-0003-9372-0655>
Ana Luiza Hoffmann Ferreira, UnB, ana.luiza.hoff@gmail.com,
<https://orcid.org/0009-0007-0474-0806>
Eduardo G. Q. Palmeira, UnB, eduardo.palmeira@unb.br,
<https://orcid.org/0000-0002-7189-8917>
Alexander E. V. Ferreira, UnB, alexander.ferreira@iadc.edu,
<https://orcid.org/0000-0001-7057-936X>
André Barros de Sales, UnB, andrebdes@unb.br,
<https://orcid.org/0000-0002-1728-6063>

Resumo: O aumento dos riscos à segurança da informação reforça a necessidade de conscientização sobre a higiene cibernética, compreendida como práticas de proteção de informações em ambientes conectados. Nesse cenário, jogos sérios (JSs) são utilizados como abordagem educativa, embora ainda haja lacunas nas práticas abordadas. Este artigo apresenta resultados de uma revisão sistemática sobre JSs voltados à higiene cibernética. Os resultados indicam o predomínio de técnicas persuasivas, como simulação, competição e recompensas, e ênfase na identificação de ameaças, enquanto práticas como *patches* e *backups* são pouco exploradas. Conclui-se que, apesar do potencial educativo dos JSs, são necessários maior diversidade de públicos-alvo, padronização de métodos de avaliação e inclusão de práticas negligenciadas.

Palavras-chave: informática na educação, jogos sérios, segurança cibernética.

The Use of Serious Games for Cyber Hygiene Education: A Systematic Review

Abstract: Increasing information security risks reinforce the need for cyber hygiene awareness, defined as information protection practices in connected environments. While serious games (SGs) are used as an educational approach, gaps persist in the practices addressed. This paper presents a systematic review of SGs focused on cyber hygiene. Findings indicate a predominance of persuasive techniques—such as simulation, competition, and rewards—and an emphasis on threat identification, while patching and backups remain under-explored. Despite the potential of SGs, greater audience diversity, standardized evaluation methods, and the inclusion of neglected practices are still required.

Keywords: computers in education, serious games, cybersecurity.

1. Introdução

A evolução das tecnologias digitais tem sido acompanhada por um aumento na diversidade das estratégias de ataques cibernéticos, exigindo novas abordagens para a proteção de dados e maior conscientização sobre segurança digital. Esses ataques comprometem a segurança de sistemas e dados, gerando impactos econômicos e sociais significativos. Financeiramente, organizações e indivíduos podem sofrer prejuízos devido a táticas como o uso de *malware* e *phishing*, resultando em custos elevados relacionados à resposta ao ataque, tempo de inatividade de serviços e danos a longo prazo, estimados em US\$ 4,88 milhões por incidente de vazamento de dados (IBM,



2024). Em termos sociais, a perda de confiança dos clientes em fornecedores de serviços e a exposição de informações pessoais confidenciais são consequências recorrentes de ataques realizados com êxito pelos invasores (DAY, 2024).

A exposição de informações pessoais durante esses incidentes pode causar danos duradouros à reputação das empresas, afetando tanto clientes existentes quanto potenciais. De acordo com o estudo de Kumari, Sinha e Priya (2014), empresas impactadas por violações de dados enfrentam um aumento médio de 5% na rotatividade de clientes, uma vez que essas violações tornam os consumidores mais exigentes quanto às garantias de proteção oferecidas. Além disso, consumidores que vivenciam violações de dados frequentemente desenvolvem ceticismo e cautela, resultando em uma redução nos volumes de transação e nas taxas de retenção. A perda de confiança pode desencadear um efeito cascata que diminui o valor da marca e a vantagem competitiva no mercado, evidenciando a necessidade urgente de medidas robustas de segurança cibernética para mitigar tais impactos.

A conscientização sobre higiene cibernética é uma das principais estratégias para mitigar os riscos de ataques. Higiene cibernética é definida como o conjunto de práticas que os usuários devem adotar para proteger a integridade de suas informações pessoais e dispositivos conectados à internet (VISHWANATH *et al.*, 2020). Exemplos dessas práticas incluem a utilização de senhas fortes, a atualização regular de softwares e a conscientização sobre táticas de *phishing*. No entanto, mesmo com usuários capacitados, a adoção consistente de práticas de higiene cibernética nem sempre ocorre, o que reforça a necessidade de treinamentos contínuos para promover mudanças efetivas (KALHORO *et al.*, 2021; HOWELL *et al.*, 2024).

A falta de higiene cibernética afeta grupos diferentes de maneira desigual. Pesquisas indicam que características demográficas, como gênero, idade e habilidades com tecnologia, podem influenciar diretamente nas práticas de segurança cibernética dos usuários (JUOZAPAVIČIUS *et al.*, 2022; BRANLEY-BELL *et al.*, 2022). Os dados apontam para a necessidade de treinamentos personalizados para diferentes grupos demográficos. Intervenções alinhadas às particularidades dos perfis dos indivíduos mostraram-se eficazes para promover comportamentos seguros entre os usuários, especialmente no que diz respeito à criação de senhas (KIOSKLI *et al.*, 2023; BUTLER; BUTLER, 2018).

Outro fator que compromete a segurança cibernética é o uso de técnicas de engenharia social por *hackers*. Eles se aproveitam de vulnerabilidades humanas, como confiança excessiva e falta de conscientização, para invadir sistemas, mesmo quando as defesas técnicas são robustas. Ataques personalizados, como o *spear phishing* — direcionado a indivíduos ou organizações específicas — e o *whaling* — que tem como alvo figuras de alto escalão, como executivos e tomadores de decisão —, tendem a ser mais eficazes, especialmente quando utilizam informações pessoais para elaborar mensagens fraudulentas altamente convincentes. Esses ataques destacam a necessidade de estratégias de segurança que não apenas foquem em aspectos técnicos, mas também considerem as vulnerabilidades comportamentais e contextuais dos usuários (SYAFITRI *et al.*, 2022).

Nesse sentido, os jogos sérios (JSs) são uma ferramenta promissora para ensinar práticas de higiene cibernética de forma interativa e engajadora, permitindo que os usuários pratiquem a identificação de ameaças em cenários realistas (FERREIRA *et al.*, 2024). Esses jogos oferecem um ambiente seguro onde os usuários podem simular ataques cibernéticos e praticar formas de defesa, construindo “hábitos ciberseguros” de maneira prática e envolvente. Para que esses jogos sejam eficazes, é fundamental que sejam projetados levando em consideração o perfil dos jogadores e que incluam



elementos que os façam se sentir imersos e ativos no processo de aprendizagem (BATTISTELLA; WANGENHEIM, 2016).

Desta forma, compreender se o perfil dos usuários contemplados nos jogos coincide com os alvos preferenciais de ataques é essencial para a criação de treinamentos eficazes. Diante desse cenário, este estudo realiza uma revisão da literatura sobre JSs voltados à higiene cibernética, examinando como o uso dessas ferramentas articula as características demográficas e comportamentais dos usuários com as estratégias de conscientização.

2. Metodologia

O presente artigo utiliza a metodologia de Revisão Sistemática (RS) para investigar na literatura sobre a aplicação de JSs no contexto da conscientização sobre segurança cibernética. Este trabalho se classifica como uma pesquisa qualitativa, bibliográfica e exploratória. Busca-se, portanto, sintetizar a literatura e contribuir para a exploração de lacunas relacionadas à higiene cibernética, avançando o conhecimento científico nessa área sem necessariamente promover aplicações práticas imediatas (GERHARDT; SILVEIRA, 2009). Seguiu-se a abordagem sistemática descrita por Kitchenham (2004) para a condução desse estudo de revisão.

2.1 Questões de Pesquisa

A formulação das questões de pesquisa (QPs) foi estruturada com base nos critérios PICO (*Population, Intervention, Comparison e Outcomes*), conforme adaptado para o contexto da Engenharia de Software por Felizardo *et al.* (2017). Nesse contexto, a população (P) é composta por usuários de JSs voltados à higiene cibernética; a intervenção (I) refere-se à avaliação das características desses jogos; a comparação (C) envolve metodologias de treinamento que não utilizam JSs, bem como as próprias características desses jogos; e o desfecho (O) buscado é a síntese de como os JSs têm sido aplicados na promoção da higiene cibernética. A partir dessa estrutura foram elaboradas as seguintes questões: **QP1:** Qual é o público-alvo de JSs que abordam segurança cibernética? **QP2:** Quais são as principais técnicas de persuasão utilizadas em treinamentos sobre segurança cibernética? **QP3:** Quais práticas de higiene cibernética são abordadas pelos JSs? **QP4:** Quais são as características dos JSs que abordam segurança cibernética?

2.2 Processo de Busca

O processo teve início com a formulação do termo de busca. Para isso, foram feitas buscas preliminares em bases bibliográficas com o termo inicial “*cybersecurity*” AND “*serious game*”, a fim de identificar palavras-chave relacionadas e refinar o termo para maior abrangência e precisão (FELIZARDO *et al.*, 2017). O termo final adotado foi: “*serious game*” AND (“*cyber hygiene*” OR “*cybersecurity awareness*” OR “*cyber security awareness*”). Este termo de busca foi, então, ajustado conforme as especificidades de cada base bibliográfica e aplicado nos campos de título, resumo e palavras-chave. Além disso, com o objetivo de ampliar o alcance da busca e incluir mais estudos sobre o tópico, o termo foi traduzido e aplicado em português; no entanto, tais buscas não retornaram resultados.

O processo de busca considerou as principais bases bibliográficas da área da computação, conforme listado por Felizardo *et al.* (2017). Apesar disso, ao final do processo, as bases efetivamente utilizadas foram: *Scopus*, *ScienceDirect*, *IEEE Xplore* e *ACM Digital Library*. Já bases como *SciELO*, *SpringerLink*, *Engineering Village* e *SBC OpenLib* foram descartadas por não retornarem resultados com o termo de busca final



ou por não permitirem busca avançada restrita aos campos de título, resumo e palavras-chave. As buscas finais foram realizadas em 23 de abril de 2024, resultando na recuperação de 45 estudos.

2.3 Seleção de Estudos

Para responder às QPs, foram selecionados estudos primários que abordam o uso de JSs no ensino de higiene cibernética (critério de inclusão). Complementarmente, aplicaram-se sete critérios de exclusão, conforme detalhado no Quadro 1:

Quadro 1 – Critérios de exclusão (CEs).

ID	Descrição
CE1	Estudo não aborda o uso de um JS para o ensino de higiene cibernética
CE2	Estudo não avalia a aplicação do JS proposto no próprio estudo
CE3	Texto completo não está disponível para acesso na internet
CE4	Artigo não é um estudo primário
CE5	Artigo não está escrito em inglês ou português
CE6	Estudo está publicado apenas como resumo
CE7	Estudo está duplicado

Esses critérios foram aplicados nas etapas de triagem, em que os estudos foram analisados com base nos títulos, resumos e palavras-chave, e de elegibilidade, na qual os estudos foram avaliados por meio da leitura dos textos completos. Na etapa de triagem, um estudo foi removido por não abordar o uso de um JS (CE1), sete por não serem estudos primários (CE4), um por não estar escrito em inglês ou português (CE5), um por ter sido publicado apenas como resumo (CE6) e onze por duplicidade (CE7); um total de 21 estudos foi excluído, resultando em 24 estudos restantes para a etapa posterior. Assim, na etapa de elegibilidade, com a análise dos textos completos, dez estudos foram removidos por não avaliarem a aplicação do JS proposto no próprio estudo (CE2). Ao final do processo de seleção, 14 estudos foram incluídos para a síntese qualitativa dessa revisão.

3. Resultados

Esta seção está organizada em subtópicos, cada um dedicado a responder uma das QPs formuladas neste estudo. As respostas foram construídas a partir da análise dos dados extraídos dos 14 trabalhos selecionados durante a condução da RS. O Quadro 2 lista os estudos incluídos para síntese qualitativa.

Quadro 2 – Lista dos artigos selecionados para a síntese qualitativa.

ID	Título	Referência
E01	Thriving in the Era of Hybrid Work: Raising Cybersecurity Awareness Using Serious Games in Industry Trainings	Zhao <i>et al.</i> (2024)
E02	A Intelligent Security Power Lab (SPL): The Ultimate Serious Game Training in Cybersecurity	Sharif e Ameen (2023)
E03	Cyber Suraksha: A Card Game for Smartphone Security Awareness	Shah e Agarwal (2023)
E04	CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness	Hodhod <i>et al.</i> (2023)
E05	AWATO: A Serious Game to Improve Cybersecurity Awareness	Ferro <i>et al.</i> (2022)
E06	Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity	Blažič e Blažič (2022)
E07	Engagement and Players' Intended Behaviors in a Cybersecurity Serious Game	Salameh e Loh (2022)
E08	Housie: A Multiplayer Game for Cybersecurity Training and Evaluation	Jayakrishnan <i>et al.</i> (2022)
E09	Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students	Qusa e Tarazi (2021)
E10	Cybersecurity Awareness Platform with Virtual Coach and Automated Challenge Assessment	Gasiba <i>et al.</i> (2020)
E11	Riskio: A Serious Game for Cyber Security Awareness and Education	Hart <i>et al.</i> (2020)
E12	Sifu - A Cybersecurity Awareness Platform with Challenge Assessment and Intelligent Coach	Gasiba, Lechner e Pinto-Albuquerque (2020)



E13	SCIPS: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control System	Cook <i>et al.</i> (2018)
E14	Design and Evaluation of a Cybersecurity Awareness Training Game	Huynh <i>et al.</i> (2017)

QP1 – Qual é o público-alvo de JSs que abordam a segurança cibernética?

A resposta a essa pergunta baseou-se na análise das descrições populacionais apresentadas nos estudos selecionados. Os dados explorados sobre a população abrangem o perfil acadêmico e profissional, a idade, a nacionalidade e o gênero dos participantes.

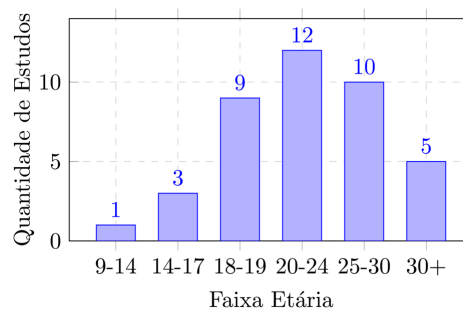
A análise dos 14 artigos sobre JSs em segurança cibernética revela um público-alvo variado, com destaque para profissionais de Tecnologia da Informação (TI) e estudantes universitários. Seis estudos envolvem profissionais de TI (E01, E08, E10, E11, E12, E13) e sete, universitários de graduação ou pós-graduação (E03, E04, E09, E10, E11, E12, E14). Também são citados estudantes do ensino fundamental e médio (E02, E06, E09), além de professores, pais e usuários diversos (E06, E07). Apenas um estudo (E05) não fornece informações específicas sobre o perfil dos participantes. O Quadro 3 sintetiza o perfil acadêmico e profissional dos participantes.

Quadro 3 – Perfil acadêmico e profissional dos participantes.

Perfil	Estudos	Percentual
Profissionais de TI	E01, E08, E10, E11, E12, E13	43%
Universitários	E03, E04, E09, E10, E11, E12, E14	50%
Estudantes do Ensino Fundamental ou Médio	E02, E06, E09	21%
Usuários Diversos	E06, E07	14%
Sem Informações Específicas	E05	7%

Quanto à faixa etária, 10 artigos investigam populações adultas (E01, E03, E04, E08, E09, E10, E11, E12, E13, E14) — três voltados exclusivamente a profissionais de TI (E01, E08, E13), quatro a universitários (E03, E04, E09, E14) e três a ambos (E10, E11, E12). Em contrapartida, outros três estudos se concentram em faixas etárias mais jovens, abrangendo alunos do ensino fundamental ao médio (E02, E06, E09); dentre esses, dois abordam também os pais e os professores dos estudantes (E02, E06). A Figura 1 ilustra a distribuição das faixas etárias identificadas.

Figura 1 – Quantidade de estudos que contemplam cada faixa etária.

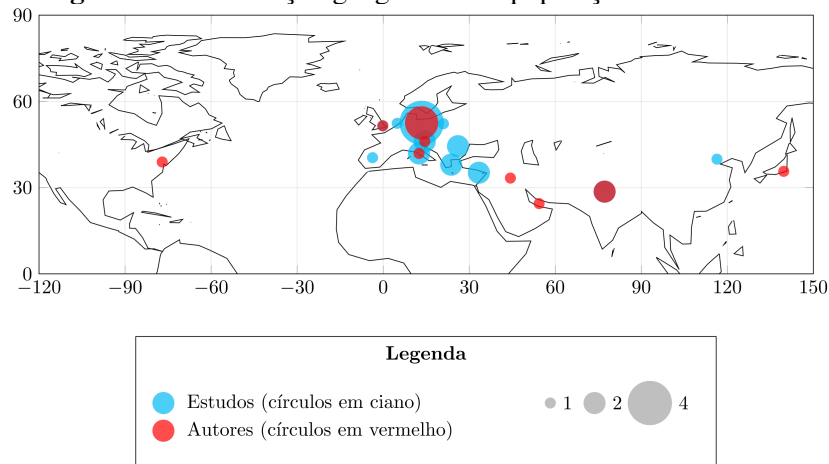


Menos da metade dos artigos analisados informa a representatividade geográfica dos participantes. Apenas seis estudos especificam a nacionalidade dos participantes: um menciona participantes internacionais de forma genérica (E07); três se concentram em indivíduos de países europeus (E02, E06, E10); outro inclui majoritariamente europeus, além de chineses e indianos (E12); e um sugere, ainda que implicitamente, a participação de estudantes universitários da Índia (E03). A ausência de estudos com populações do hemisfério sul levou à escolha de representar apenas o hemisfério norte na Figura 2.

A revisão dos artigos indica um perfil majoritariamente masculino entre os participantes dos estudos sobre JSs em segurança cibernética, conforme apontado em cinco estudos (E03, E04, E05, E07, E08). Em contraste, dois trabalhos registram

predominância feminina (E02, E06). Vale destacar que, em um dos estudos, uma minoria dos participantes se identifica com outros gêneros ou opta por não declarar, representando menos de 2% do total de participantes desse mesmo estudo (E08).

Figura 2 – Distribuição geográfica das populações encontradas.



A maioria dos estudos não fornece informações detalhadas sobre a experiência dos participantes com computadores. Apenas um artigo apresenta dados quantitativos, indicando que a maioria se considera com nível intermediário (E05). No entanto, a ausência de outros dados demográficos — como ocupação, formação, idade e gênero — nesse estudo limita possíveis correlações entre as experiências e as características dos participantes.

QP2 – Quais são as principais técnicas de persuasão utilizadas em treinamentos sobre segurança cibernética?

Para responder a essa questão, analisou-se a ocorrência de diferentes técnicas de persuasão nos artigos selecionados para esta revisão. As técnicas identificadas foram classificadas segundo as categorias proposta por Orji, Nacke e Di Marco (2017): competição, simulação, automonitoramento e feedback, recompensa, comparação, cooperação, punição, definição de metas e sugestão, personalização e customização — os nomes das técnicas são traduções livres dos autores para o português. Em JSs, essas estratégias buscam engajar usuários por meio da aprendizagem ativa e promover mudanças efetivas de comportamento em relação à segurança cibernética. O Quadro 4 apresenta as técnicas identificadas nos estudos e sintetiza como foram aplicadas.

Quadro 4 – Técnicas identificadas nos estudos analisados.

Técnica	Aplicação	Estudos	Percentual
Competição	Essa técnica envolveu a criação de um ambiente competitivo, incentivando os participantes a competirem entre si, o que aumentou o engajamento e motivou a aprendizagem	E01, E06, E08, E13	29%
Simulação	A técnica de simulação foi utilizada para recriar cenários realistas em que os usuários podiam praticar suas habilidades	E01, E05, E06, E07, E09, E13	43%
Automonitoramento e Feedback	O automonitoramento permitiu que os participantes acompanhassem seu progresso, enquanto o feedback forneceu orientação para melhorarem seu desempenho	E05, E06, E13	21%
Recompensa	Recompensas, como moedas, foram utilizadas para motivar os usuários a continuarem se empenhando em suas tarefas e comprarem itens disponíveis no jogo	E06, E08, E10, E13	29%
Comparação	Essa técnica permitiu que os participantes comparassem seus desempenhos com os de outros grupos ou jogadores, promovendo o aprendizado coletivo e o engajamento	E03, E11, E13	21%
Cooperação	A cooperação foi usada para estimular o trabalho em equipe, onde os participantes precisaram colaborar para alcançar um objetivo comum	E03, E11, E13	21%



Punição	Essa técnica foi utilizada para desencorajar comportamentos inadequados, impondo consequências para erros cometidos durante os treinamentos	E13, E14	14%
Definição de Metas e Sugestão	Essa técnica foi observada em um artigo relacionado a práticas como captura à bandeira	E10	7%
Personalização	A personalização foi destacada em um artigo onde os conteúdos foram adaptados de acordo com as necessidades e características específicas dos participantes	E04	7%
Customização	Essa técnica não foi explicitamente mencionada nos artigos analisados	Nenhum	0%

A simulação foi a técnica mais frequente (43%), seguida por competição e recompensa (29% cada). As técnicas menos utilizadas foram comparação e cooperação (21% cada), punição (14%), definição de metas e sugestão, e personalização (7% cada). A customização não foi identificada em nenhum estudo, e um artigo (E12) não mencionou nenhuma das técnicas de persuasão investigadas. Observou-se que essas técnicas são frequentemente aplicadas de forma combinada nos JSs, sugerindo que programas de treinamento em higiene cibernética podem se beneficiar da integração de múltiplas abordagens persuasivas para promover mudanças comportamentais efetivas.

QP3 – Quais práticas de higiene cibernética são abordadas pelos JSs?

As práticas de higiene cibernética foram identificadas nos artigos selecionados seguindo a classificação de Singh *et al.* (2020): identificar, priorizar, melhorar segurança, *patches* de segurança, *backup* e treinamento efetivo — termos traduzidos livremente pelos autores. O Quadro 5 identifica e apresenta tais atividades nos estudos analisados.

Quadro 5 – Práticas de higiene cibernética abordadas pelos jogos

Prática	Descrição	Estudos	Percentual
Identificar	Capacidade de distinguir dispositivos e perigos digitais em intervalos constantes	E02, E03, E04, E06, E07, E10, E11, E14	57%
Priorizar	Classificação e categorização de dispositivos e aplicativos com base na sensibilidade e exposição de dados	E06, E13	14%
Melhorar Segurança	Fortalecimento de dispositivos, <i>frameworks</i> e aplicativos para garantir a segurança e diminuir os pontos de entrada para ataques digitais. Isso inclui a encriptação das informações, avaliações de vulnerabilidade, auditorias de configuração segura, políticas de senhas e autenticação de dois fatores	E01, E04, E06, E07, E10, E11, E13	50%
<i>Patches</i> de Segurança	Execução de <i>patches</i> e administração de fraquezas em todos os dispositivos e <i>frameworks</i> , mantendo as atualizações em dia contra ameaças recentes ou comuns	E01, E04, E10	21%
<i>Backup</i>	A incorporação de um processo de recuperação garante que, em caso de incidentes, a perda de informações ou estados do sistema possa ser revertida — depender de <i>backups</i> é a última defesa contra a perda ou roubo de informações	Nenhum	0%
Treinamento Efetivo	A prática mais econômica de higiene cibernética. Por meio dos diversos métodos de treinamento é possível capacitar indivíduos e equipes, promovendo uma conscientização que serve como primeira linha de defesa contra-ataques	E01, E05, E06, E08, E09, E13	43%

O Quadro 5 mostra que metade dos artigos abordam ao menos duas atividades de higiene cibernética. As práticas mais frequentes foram identificar (57%), melhorar segurança (50%) e treinamento efetivo (43%), enquanto *patches* de segurança (21%) e priorizar (14%) receberam menos atenção. A prática de *backup* não foi mencionada nos estudos, e um artigo (E12) não abordou explicitamente nenhuma das práticas listadas.

Os resultados indicam ênfase na identificação de ameaças, fortalecimento da segurança e treinamento de usuários. As práticas menos abordadas sugerem possíveis lacunas no gerenciamento de vulnerabilidades e aplicação de correções. A ausência de menções ao *backup* nos treinamentos levanta questões sobre a integração de práticas cotidianas nos métodos de higiene cibernética, podendo refletir diferentes fatores como



automação desses processos, políticas organizacionais centralizadas ou atribuição específica a gestores, aspectos que merecem investigação futura.

QP4 – Quais são as características dos JSs que abordam segurança cibernética?

Os dados coletados foram agrupados por similaridade temática, resultando em oito características dos JSs: interação entre jogadores, narrativa, avaliação, duração, pré-requisitos conceituais, modelos de design, tecnologias de desenvolvimento e recursos necessários. Cada aspecto será detalhado nos tópicos seguintes.

Interação entre os jogadores: Dos 14 estudos analisados, 13 mencionam o tipo de interação entre jogadores. Sete estudos utilizam modo *mono-player*, onde o usuário participa individualmente do treinamento por meio de um JS (E02, E04, E05, E07, E09, E10, E14), e seis adotam modo *multi-player*, envolvendo interação entre dois ou mais jogadores (E01, E03, E08, E11, E12, E13). Entre os jogos *multi-player*, um estudo menciona uma colaboração entre os jogadores como “suave” (E12), dois descrevem jogos competitivos (E01, E08), e um apresenta elementos mistos competitivos-colaborativos (E13).

Narrativa: Para definir os tipos de narrativas presentes nos JSs, foram utilizadas as definições de De Lope e Medina-Medina (2017), categorizando-as com base no espaço que ocupam. Distinguem-se quatro tipos: histórias evocativas (histórias navegáveis já conhecidas), histórias encenadas (foco em atingir objetivos com possíveis micronarrativas emocionais), histórias incorporadas (narrativa integrada aos elementos do cenário) e histórias emergentes (jogador é responsável pela construção da história). Dos 14 artigos analisados, três não fazem menção detalhada sobre a narrativa presente no JS associado (E06, E08, E12). Um estudo menciona múltiplas categorias (histórias evocativas, encenadas e incorporadas) (E02), quatro estudos mencionam histórias encenadas (E01, E09, E10, E14), outros quatro estudos mencionam histórias incorporadas (E03, E05, E07, E13) e dois estudos mencionam histórias emergentes (E04, E11).

Avaliação dos jogadores: Um artigo não detalha o tipo de avaliação realizada sobre o desempenho dos jogadores (E06). Dentre os 13 restantes, apenas três avaliam os jogadores de forma manual durante o treinamento (E03, E11, E13). Nove estudos relatam a realização de avaliações de forma automática (E01, E04, E05, E07, E08, E09, E10, E12, E14) e um relata misturar avaliações manuais e automáticas (E02). Dos 13 artigos, dez mencionam avaliação durante o treinamento, frequentemente combinada com outra avaliação posterior. Avaliações prévias ao treinamento são menos comuns, aparecendo em apenas dois estudos (E02, E09).

Tempo de duração do treinamento: O tempo de duração de uma partida ou seção é mencionado em metade dos estudos analisados. Os treinamentos costumam ter duração de 15 a 60 minutos (E01, E03, E07, E10, E11), podendo variar de acordo com o grupo que irá participar do jogo. Dois estudos divergem dessa faixa temporal, com durações de aproximadamente 90 minutos (E13) e 5 minutos (E09). Geralmente, os JSs oferecem treinamento rápido em segurança cibernética e permitem uso por diferentes períodos mediante reaplicação. A maioria das durações mencionadas referem-se ao tempo por sessão, não ao tempo total do treinamento.

Pré-requisitos conceituais: É fundamental alinhar o treinamento ao conhecimento prévio e experiência prática dos participantes. Essa adequação ao público-alvo torna o treinamento mais relevante e engajador, despertando interesse no desenvolvimento das habilidades propostas (REIGELUTH, 1999). Apesar da importância dos pré-requisitos conceituais, apenas oito estudos os mencionam. Seis indicam que não são necessários conhecimentos prévios sobre os assuntos do



treinamento (E01, E02, E03, E05, E09, E11), enquanto um exige conhecimento sobre contexto histórico (E13) e outro demanda conhecimentos técnicos em segurança cibernética, como nomenclaturas e tipos de ataques (E08).

Modelos de design: Os modelos de design foram mencionados em seis artigos, geralmente de forma sucinta. Os modelos identificados foram: *Action Design Research (ADR) Method* (E01); *Conceptual Framework* (E03); *Stenmap Framework* (E04); *STRIDE Threat Taxonomy* (E11); *5 Spectrums* (E13); e *Activity Theory-based Model of Serious Game (ATMSG)* (E14). Como cada modelo aparece apenas uma vez, não foi possível identificar padrões de uso. Estudos futuros podem investigar como cada modelo atua e suas possíveis correlações.

Tecnologias de desenvolvimento: Entre os 14 jogos analisados, dois são físicos (jogos de cartas) (E03, E11), onze são jogos digitais (E01, E02, E04, E05, E06, E07, E08, E09, E10, E12, E14) e um combina elementos físicos e digitais (E13). Dos digitais, dois utilizam plataforma *web* (E08, E09), sendo que um deles também é compatível com *mobile* (E08), e nove não especificam explicitamente a plataforma (E01, E02, E04, E05, E06, E07, E10, E12, E14). Cinco estudos mencionam as tecnologias de desenvolvimento utilizadas: *Unity, C#* (E04); *Unreal Engine, Blueprints, C++* (E05); *Spring Boot, IntelliJ, React JS, VSCode* (E08); *Construct3 Dev Kit, HTML5, Javascript plugins* (E09); e *Python 3.8, Flask* (E10). Observa-se, portanto, uma preferência dos desenvolvedores por ambientes digitais nos treinamentos de segurança cibernética. No entanto, as tecnologias identificadas não revelam padrões ou preferências consistentes entre os desenvolvedores.

Recursos necessários para o treinamento: Informações sobre disponibilidade dos jogos em plataformas de distribuição e requisitos de equipamentos são escassas nos artigos. Embora mencionem a necessidade de internet, nenhum estudo detalha requisitos de *hardware* e *software*. Para jogos físicos, são citados recursos como cartas, tabuleiros e mesas, além da necessidade de uma pessoa experiente para atuar como mediadora ou guia no treinamento (E03, E11).

4. Discussão

Embora a análise dos estudos evidencie o potencial educativo dos JSs no ensino de higiene cibernética, observam-se limitações metodológicas que podem comprometer sua eficácia e aplicabilidade em contextos mais amplos. A eficácia dos achados é limitada pela baixa diversidade demográfica e geográfica, com amostras concentradas em estudantes e profissionais de TI europeus do gênero masculino. A sub-representação de grupos como estudantes do ensino médio, professores ou usuários de diferentes contextos culturais, e a escassez de dados sobre a nacionalidade dos participantes dificultam a generalização dos resultados para diferentes contextos socioculturais e socioeconômicos.

Outro aspecto crítico observado é a ausência de abordagens específicas para práticas técnicas essenciais (SINGH *et al.*, 2020), como aplicação de *patches* de segurança e realização de *backups*, aspectos negligenciados nas narrativas e dinâmicas dos jogos analisados. Incorporar essas práticas poderia ampliar a abrangência e eficácia educacional, promovendo maior conscientização sobre medidas preventivas no fortalecimento da segurança digital. Em contraste, práticas como identificação de ameaças e treinamento de habilidades básicas receberam maior atenção, indicando uma ênfase desproporcional em aspectos introdutórios da higiene cibernética.

As interações *mono-player* e *multi-player*, narrativas baseadas em histórias evocativas, emergentes ou incorporadas (DE LOPE; MEDINA-MEDINA, 2017), e técnicas de persuasão como simulação, competição e recompensas (ORJI; NACKE; DI



MARCO, 2017) demonstraram relevância para o engajamento e interesse dos jogadores. Por outro lado, a ausência de padronização na avaliação dos jogos compromete a comparabilidade entre estudos, dificultando a identificação de melhores práticas. Poucos realizaram avaliações pré e pós-jogo, e menos ainda aplicaram reavaliações periódicas para medir retenção do aprendizado. Observou-se também grande variação na duração das partidas — de cinco minutos a mais de uma hora. Embora essa diversidade seja positiva para adaptar os jogos a diferentes contextos, a falta de informações sobre duração em metade dos estudos prejudica a replicação prática e adequação às necessidades específicas de treinamento.

Com base nessas observações, propõem-se diversas melhorias para a concepção e avaliação de JSs em higiene cibernética. Primeiramente, recomenda-se a padronização de critérios de avaliação e categorização, abrangendo práticas técnicas, impacto educacional e engajamento do usuário. A realização de avaliações pré e pós-jogo, acompanhadas de reavaliações periódicas, é essencial para medir a retenção do conhecimento e avaliar mudanças comportamentais. Além disso, a diversificação dos públicos estudados, incluindo faixas etárias mais jovens e populações culturalmente diversas, é fundamental para ampliar a aplicabilidade dos resultados.

A metodologia de *debriefing* destacou-se como uma abordagem essencial ao proporcionar um espaço para reflexão e consolidação ativa do conhecimento adquirido. Contudo, a eficácia desses jogos depende da sua capacidade de incorporar princípios como *feedback* imediato e adequação às necessidades específicas dos usuários (FERREIRA *et al.*, 2024). Portanto, estudos futuros devem explorar a relação entre narrativas, interações nos jogos e técnicas de persuasão, buscando identificar combinações mais eficazes para diferentes perfis de jogadores.

Por fim, o desenvolvimento de jogos com conteúdos personalizados para públicos específicos e que integrem práticas técnicas negligenciadas, como *backup* e *patches* de segurança, poderá contribuir significativamente para a efetividade dessas ferramentas no ensino de higiene cibernética. A implementação dessas estratégias tem potencial para avançar o uso de JSs como instrumentos educativos, promovendo uma cultura global de segurança digital mais sólida e abrangente.

5. Conclusões

Este estudo investigou o uso de JSs para o ensino de práticas de higiene cibernética por meio de uma RS com o objetivo de identificar características, limitações e oportunidades de aprimoramento. A análise revelou que os JSs têm potencial para engajar usuários e promover aprendizado; no entanto, carecem de maior abrangência em termos demográficos e geográficos (KALHORO *et al.*, 2021; VISHWANATH *et al.*, 2020). Além disso, práticas fundamentais como *backups* e aplicação de *patches* são raramente abordadas enquanto técnicas como simulação e competição predominam (SINGH *et al.*, 2020; ORJI; NACKE; DI MARCO, 2017).

Como contribuição, o trabalho destacou a importância de alinhar os jogos às necessidades dos usuários, integrando práticas negligenciadas e diversificando públicos-alvo. Recomenda-se também a padronização de critérios de avaliação para aumentar a comparabilidade entre estudos (KITCHENHAM, 2004; DE LOPE; MEDINA-MEDINA, 2017). Estudos futuros devem investigar jogos com narrativas personalizadas e práticas técnicas expandidas, além de conduzir avaliações longitudinais sobre retenção de conhecimento e mudanças comportamentais (REIGELUTH, 1999; ZHAO *et al.*, 2024). Tais esforços fortalecerão o papel dos JSs na educação em segurança cibernética.

Referências Bibliográficas

- BATTISTELLA, P. E.; WANGENHEIM, C. G. von. Games for Teaching Computing in Higher Education – A Systematic Review. *IEEE Technology and Engineering Education (ITEE)*, v. 1, n. 3, p. 8–30, 2016. Disponível em: [Link](#).
- BLAŽIČ, B. J.; BLAŽIČ, A. J. Cybersecurity Skills among European High-School Students: A New Approach in the Design of Sustainable Educational Development in Cybersecurity. *Sustainability*, v. 14, n. 8, p. 1–23, 2022. DOI: [10.3390/su14084763](#).
- BRANLEY-BELL, D.; COVENTRY, L.; DIXON, M.; JOINSON, A.; BRIGGS, P. Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*, v. 2022, p. 1–10, 2022. DOI: [10.1155/2022/2693080](#).
- BUTLER, R.; BUTLER, M. Some password users are more equal than others: Towards customisation of online security initiatives. *South African Journal of Information Management*, v. 20, n. 1, p. 1–10, 2018. DOI: [10.4102/sajim.v20i1.920](#).
- COOK, A.; SMITH, R. G.; MAGLARAS, L.; JANICKE, H. SCIPS: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control System. *International Journal of Cyber Warfare and Terrorism*, v. 7, n. 2, p. 1–15, 2017. DOI: [10.4018/IJCWT.2017040101](#).
- DAY, B. Guide to Understanding & Protecting Against DDoS Attacks. *Guardian Digital*, 14 de março de 2024. Disponível em: [Link](#). Acesso em: 18 jul. 2024.
- DE LOPE, R. P.; MEDINA-MEDINA, N. A Comprehensive Taxonomy for Serious Games. *Journal of Educational Computing Research*, v. 55, n. 5, p. 629–672, 2017. DOI: [10.1177/0735633116681301](#).
- FELIZARDO, K. R.; NAKAGAWA, E. Y.; FABBRI, S. C. P. F.; FERRARI, F. C. *Revisão Sistemática da Literatura em Engenharia de Software: Teoria e Prática*. 1. ed. Rio de Janeiro: Elsevier, 2017.
- FERREIRA, A. L. H.; SALES, A. B. de; FERREIRA, A. E. V.; PALMEIRA, E. G. Q. Características dos jogos sérios Anti-Phishing como ferramenta de ensino: uma revisão sistemática. *RENOTE*, Porto Alegre, v. 22, n. 1, p. 340–350, 2024. DOI: [10.22456/1679-1916.141560](#).
- FERRO, L. S.; MARRELLA, A.; CATARCI, T.; SAPIO, F.; PARENTI, A.; DE SANTIS, M. AWATO: A Serious Game to Improve Cybersecurity Awareness. In: FANG, X. (org.). HCI in Games. HCII 2022. *Lecture Notes in Computer Science*, v. 13334. Cham: Springer, 2022. p. 508–529. DOI: [10.1007/978-3-031-05637-6_33](#).
- GASIBA, T. E.; LECHNER, U.; PINTO-ALBUQUERQUE, M. Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, v. 3, n. 24, p. 1–23, 2020. DOI: [10.1186/s42400-020-00064-4](#).
- GASIBA, T.; LECHNER, U.; PINTO-ALBUQUERQUE, M.; PORWAL, A. Cybersecurity Awareness Platform with Virtual Coach and Automated Challenge Assessment. In: KATSIKAS, S. et al. (org.). *Lecture Notes in Computer Science*, v. 12501. Cham: Springer, 2020. p. 67–83. DOI: [10.1007/978-3-030-64330-0_5](#).
- GERHARDT, T. E.; SILVEIRA, D. T. (org.). *Métodos de Pesquisa*. 1. ed. Porto Alegre: Editora da UFRGS, 2009.
- HART, S.; MARGHERI, A.; PACI, F.; SASSONE, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, v. 95, p. 1–16, 2020. DOI: [10.1016/j.cose.2020.101827](#).
- HODHOD, R.; HARDAGE, H.; ABBAS, S.; ALDAKHEEL, E. A. CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics*, v. 12, n. 17, p. 1–18, 2023. DOI: [10.3390/electronics12173544](#).
- HOWELL, C.; MAIMON, D.; MUNIZ, C.; KAMAR, E.; BERENBLUM, T. Engaging in cyber hygiene: the role of thoughtful decision-making and informational interventions. *Frontiers in Psychology*, v. 15, p. 1–11, 2024. DOI: [10.3389/fpsyg.2024.1372681](#).
- HUYNH, D.; LUONG, P.; IIDA, H.; BEURAN, R. Design and Evaluation of a Cybersecurity Awareness Training Game. In: MUNEKATA, N.; KUNITA, I.; HOSHINO, J. (org.). *Lecture Notes in Computer Science*, v. 10507. Cham: Springer, 2017. p. 183–188. DOI: [10.1007/978-3-319-66715-7_19](#).

- IBM. Cost of a Data Breach Report 2024. *IBM*, 2024. Disponível em: [Link](#). Acesso em: 21 dez. 2024.
- JAYAKRISHNAN, G. C.; BANAHATTI, V.; LODHA, S.; SIRIGIREDDY, G.; NIVAS, S. Housie: A Multiplayer Game for Cybersecurity Training and Evaluation. In: 2022 ANNUAL SYMPOSIUM ON COMPUTER-HUMAN INTERACTION IN PLAY (CHI PLAY '2022), 2022, Bremen, Alemanha. *Extended Abstracts of the [...]*. Nova Iorque: Association for Computing Machinery, 2022. p. 17–23. DOI: [10.1145/3505270.3558328](#).
- JUOZAPAVIČIUS, A.; BRILINGAITĖ, A.; BUKAUSKAS, L.; LUGO, R. G. Age and Gender Impact on Password Hygiene. *Applied Sciences*, v. 12, n. 2, p. 1–15, 2022. DOI: [10.3390/app12020894](#).
- KALHORO, S.; REHMAN, M.; PONNUSAMY, V.; SHAIKH, F. B. Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access*, v. 9, p. 99339–99363, 2021. DOI: [10.1109/ACCESS.2021.3097144](#).
- KITCHENHAM, B. *Procedures for Performing Systematic Reviews*. 2004. Keele University Technical Report TR/SE-0401. Disponível em: [Link](#).
- KIOSKLI, K.; FOTIS, T.; NIFAKOS, S.; MOURATIDIS, H. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences*, v. 13, n. 6, p. 1–16, 2023. DOI: [10.3390/app13063410](#).
- KUMARI, M.; SINHA, P. C.; PRIYA, S. The Impact of Data Breaches on Consumer Trust in E-Commerce. *International Journal of Current Science*, v. 4, n. 4, p. 1–9, 2014. DOI: [10.1729/Journal.41016](#).
- ORJI, R.; NACKE, L. E.; DI MARCO, C. Towards Personality-driven Persuasive Health Games and Gamified Systems. In: 2017 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI '17), 2017, Denver, Colorado, EUA. *Proceedings of the [...]*. Nova Iorque: Association for Computing Machinery, 2017. p. 1015–1027. DOI: [10.1145/3025453.3025577](#).
- QUSA, H.; TARAIZI, J. Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. In: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, Nevada, EUA. *Proceedings of the [...]*. IEEE, 2021. p. 677–682. DOI: [10.1109/CCWC51732.2021.9375847](#).
- REIGELUTH, C. M. *Instructional-design Theories and Models: A New Paradigm of Instructional Theory*. 1. ed. Nova Iorque: Routledge, 1999.
- SALAMEH, R.; LOH, C. S. Engagement and Players' Intended Behaviors in a Cybersecurity Serious Game. *International Journal of Gaming and Computer-Mediated Simulations*, v. 14, n.1, p. 138–158, 2022. DOI: [10.4018/IJGCMS.313185](#).
- SHAH, P.; AGARWAL, A. Cyber Suraksha: a card game for smartphone security awareness. *Information and Computer Security*, v. 31, n. 5, p. 576–600, 2023. DOI: [10.1108/ICS-05-2022-0087](#).
- SHARIF, K. H.; AMEEN, S. Y. A Intelligent Security Power Lab (SPL): The Ultimate Serious Game Training in Cybersecurity. *International Journal of Intelligent Systems and Applications in Engineering*, v. 11, n. 11s, p. 245–259, 2023. Disponível em: [Link](#).
- SINGH, D.; MOHANTY, N. P.; SWAGATIKA, S.; KUMAR, S. Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Engineering and Management*, v. 83, p. 8145–8152, 2020. Disponível em: [Link](#).
- SYAFITRI, W.; SHUKUR, Z.; MOKHTAR, U. A.; SULAIMAN, R.; IBRAHIM, M. A. Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, v. 10, p. 39325–39343, 2022. DOI: [10.1109/ACCESS.2022.3162594](#).
- VISHWANATH, A.; NEO, L. S.; GOH, P.; LEE, S.; KHADER, M.; ONG, G.; CHIN, J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, v. 128, p. 1–11, 2020. DOI: [10.1016/j.dss.2019.113160](#).
- ZHAO, T.; GASIBA, T.; LECHNER, U.; PINTO-ALBUQUERQUE, M. Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. *Journal of Systems and Software*, v. 210, p. 1–22, 2024. DOI: [10.1016/j.jss.2023.111946](#).