We Got Hacked! - Simulador de treinamento para aprendizado de resposta a incidentes de segurança cibernética

Rodrigo Steigleder[1], Luciano Ignaczak[1], Mauricio Bammann Gehling[1], Frank Vega Gonçalves[1], Jairo Augusto de Campos Alff[1], Nicolay Hoff[1] Tiago Umberto Gazzola[1]

[1]Universidade do Vale do Rio dos Sinos - Unisinos, Av. Unisinos, 950, São Leopoldo, RS, 93022-750, Brasil.

{lignaczak,mgehling}@unisinos.br,

{rosteigleder,goncalvesfrank,jairoalff,nicolayh,tiagoug}@edu.unisinos.br

Abstract. *The growing number of cyber incidents underscores the need for effective methodologies to train incident response teams. Given the shortage of educational games in Portuguese that simulate the daily routine of a Security Operations Center (SOC), We Got Hacked! was developed to support the training of students and professionals. This article summarizes the game's development process and reports the results of an external evaluation conducted in 2026, focusing on participants' experience. The findings indicate: (i) high ratings for relevance, enjoyment, and satisfaction; and (ii) opportunities for improvement, particularly the implementation of a progress-saving feature.*

Resumo. *O aumento dos incidentes cibernéticos evidencia a necessidade de metodologias para a capacitação de times que atuam em resposta a incidentes. Frente à lacuna de jogos educacionais em língua portuguesa que simulam o cotidiano de um Centro de Operações de Segurança (SOC), o projeto We Got Hacked! apresenta-se como uma opção para a qualificação de estudantes e profissionais. Este artigo sintetiza o ciclo de desenvolvimento da ferramenta e apresenta a avaliação externa realizada em 2026, focada na experiência dos participantes. Os resultados indicaram: (i) altas pontuações nas categorias de relevância, diversão e satisfação; e (ii) a necessidade de ajustes, como a criação da funcionalidade de salvamento do progresso.*

1. Introdução

As organizações operam em um ambiente de constante exposição a ataques cibernéticos (CHECK POINT, 2026), cujo impacto financeiro pode alcançar patamares superiores a 4 milhões de dólares (IBM, 2025). Para enfrentar esse cenário, é desejável a estruturação de times de resposta a incidentes (CSIRTs), os quais coordenam e desenvolvem diversas ações de mitigação para conter e recuperar ambientes computacionais impactados por incidentes cibernéticos[1]. Essas equipes podem atuar em conjunto com unidades que monitoram e detectam as ameaças, conhecidas como Centros de Operações de Segurança (SOC)[2].

[1]https://csrc.nist.gov/glossary

[2]https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

O panorama de ameaças é agravado pela inexperiência de uma parcela significativa dos profissionais da área, onde estima-se que 44% das equipes de segurança sejam compostas por membros com menos de três anos de atuação (ISACA, 2023). Diante desse desafio, jogos educacionais têm demonstrado potencial ao prover ambientes controlados para o desenvolvimento de competências técnicas e autoconfiança em segurança cibernética (Pérez; Castro; López, 2023; Angafor; Yevseyeva; Maglaras, 2024; Pirta-Dreimane et al., 2024), consolidando-se como uma ferramenta eficiente de treinamento para esse campo de estudos (Khando et al., 2021).

Apesar dos avanços observados no campo de jogos educacionais, a literatura científica aponta uma carência de ferramentas em língua portuguesa voltadas especificamente para a simulação de resposta a incidentes. Buscando preencher essa lacuna, este trabalho apresenta o We Got Hacked!, um jogo projetado para capacitar estudantes e profissionais por meio da simulação da rotina de um SOC. O jogo foi desenvolvido entre janeiro de 2025 e julho de 2026 por um grupo multidisciplinar que respondeu ao edital do Programa Hackers do Bem da RNP[3]. Este artigo descreve a visão geral da solução e suas funcionalidades, além de analisar os resultados alcançados no estudo realizado em janeiro de 2026, focado na experiência do usuário.

Este trabalho está organizado da seguinte forma: a Seção 2 aborda o estado da arte em jogos educacionais direcionados à segurança cibernética. A Seção 3 apresenta as funcionalidades do jogo desenvolvido. A Seção 4 documenta a metodologia utilizada na avaliação externa realizada em janeiro de 2026. Na seção 5 são discutidos os resultados obtidos na avaliação. Por fim, a Seção 6 apresenta as conclusões, futuras pesquisas e limitações deste estudo.

2. Trabalhos Relacionados

Os autores aplicaram uma metodologia de revisão sistemática da literatura, seguindo um protocolo baseado no *framework* de Kitchenham, Budgen e Brereton (2015). Para a obtenção dos trabalhos, foram selecionadas as bases de dados científicas Emerald[4], IEEE Xplore[5], Science Direct[6], Springer[7], Taylor & Francis[8] e Wiley[9]. A pesquisa considerou artigos publicados a partir de 2020 e uma *string* de busca que considerou palavras-chaves dos três tópicos principais: segurança cibernética (*cyber security, cybersecurity, information security*), área de resposta a incidentes (*incident response*) e modelos de aprendizado (*gamified, gamefication, serious games, interactive learning, education game*). A string foi configurada com o operador "AND" entre os tópicos e o operador "OR" entre as palavras-chaves.

Dentre os 62 artigos inicialmente mapeados em janeiro de 2025, oito foram selecionados para análise. A avaliação da literatura corrobora o impacto positivo de métodos de simulação no aprimoramento de competências em segurança cibernética. Estudos indicam a utilização de jogos de cartas e exercícios de *tabletop* remotos para aumentar

[3]https://www.rnp.br/projetos/hackers-do-bem/
[4]https://www.emerald.com/insight/
[5]https://ieeexplore.ieee.org/Xplore/home.jsp
[6]https://www.sciencedirect.com/
[7]https://link.springer.com/
[8]https://www.tandfonline.com/
[9]https://onlinelibrary.wiley.com/

a conscientização sobre a postura corporativa em relação a riscos cibernéticos (Angafor; Yevseyeva; Maglaras, 2024, 2023). Adicionalmente, o trabalho de Pirta-Dreimane et al. (2024) implementou um jogo de *escape room*, evidenciando que fatores emocionais e comportamentais são relevantes para a resolução de problemas em cenários realistas.

Já a pesquisa de Hatzivasilis et al. (2021) avaliou uma plataforma online de emulação e simulação de ataques, concluindo que treinamentos customizáveis preparam os participantes para mitigar incidentes em condições reais. Outros estudos exploraram a tomada de decisão em segurança ofensiva e em resposta a incidentes (Katsantonis; Mavridis; Gritzalis, 2021; O'Connor et al., 2021), além da aplicação de jogos no ensino fundamental (Videnovik; Filiposka; Trajkovik, 2024), enquanto pesquisas como a de Tharot et al. (2023) reforçam a necessidade de sequências pedagógicas estruturadas para o setor industrial.

A análise dos trabalhos indica uma predominância de soluções voltadas à conscientização e à simulação de ataques cibernéticos. Em relação à área de resposta a incidentes, os jogos restringem-se a formatos como *tabletop*, jogos físicos ou exercícios remotos. Embora trabalhos como o de O'Connor et al. (2021) explorem a tomada de decisão, observa-se a ausência de soluções digitais que integrem o fluxo de trabalho de uma equipe de resposta a incidentes. Diante deste cenário e da ausência de aplicações desenvolvidas na língua portuguesa, o We Got Hacked! posiciona-se como uma solução inovadora, introduzindo os conceitos de resposta a incidentes e simulando as atividades cotidianas de um SOC.

3. O We Got Hacked!

O We Got Hacked! é um jogo educacional em língua portuguesa, no formato *single-player*, desenvolvido como aplicação *web* em Unity[10]. O projeto é fruto de uma iniciativa que criou um grupo de trabalho multidisciplinar, envolvendo professores, alunos e egressos dos cursos de graduação em Jogos Digitais e Segurança da Informação, da UNISINOS. Seu objetivo é desenvolver o raciocínio crítico e a agilidade na tomada de decisão, capacitando estudantes e profissionais em resposta a incidentes cibernéticos por meio de um ambiente que simula a rotina de um SOC. A seguir, esta seção detalha as funcionalidades presentes na versão do jogo de julho de 2026.

A narrativa central explora o conflito entre a organização petrolífera PetroCAIS e o grupo hacktivista PetroKillers. O jogador integra a equipe de resposta a incidentes da C.A.F.E., empresa especializada em segurança cibernética contratada para defender os sistemas da PetroCAIS. Ao longo do jogo, é possível assumir diferentes papéis técnicos, como os de Raquel (gerente do SOC), Tiago (analista N1), Rafael (analista N2) e Eduardo (analista N3). Além da equipe operacional da C.A.F.E., o jogador interage com personagens que compõem o quadro da PetroCAIS, incluindo Gustavo (gerente de TI), Thayná (relações públicas) e André (diretor jurídico). Para conferir maior imersão e realismo, todos os personagens possuem um perfil comportamental definido, que abrange desde a postura e modo de se expressar até o estilo de vestimenta.

A partir da narrativa estabelecida, a experiência do jogo foi estruturada em três fases, cada qual representando um cenário de incidente cibernético com níveis de complexidade crescentes. As fases abrangem ataques de pichação de site (*defacement*) e *ransomware*,

[10]https://unity.com/

além de um vazamento de dados. O objetivo é garantir que o treinamento evolua dos conceitos de detecção e triagem básica até a gestão de crises cibernéticas. A primeira fase do jogo simula um ataque de *defacement* ao site da PetroCAIS. Para resolver o incidente, o jogador deve tomar decisões, guiado por um *playbook* e pela troca de mensagens entre os personagens. As mecânicas de *gameplay* garantem a progressão das ações, integrando ferramentas de segurança que simulam aplicações reais, entre elas, um sistema centralizador de *logs* (chamado de SIEMtinel), um cliente de e-mail (ANEXUS Mail), uma aplicação de gerenciamento de *tickets* (Tick Task) e um utilitário que permite a restauração de *backup* do site (Desconex).

A segunda fase introduz um ataque de *ransomware* originado de um *phishing* enviado à empresa petrolífera. O jogador precisa investigar a estrutura do cliente para confirmar o ataque e registrar o incidente. Na sequência, deve gerir a crise em uma sala de guerra, identificar a causa raiz do ataque, aplicar correções e restaurar dados. Neste incidente, além das ferramentas anteriores, o ambiente apresenta novos recursos: o software de conexão remota (chamado de Remotinik), a aplicação que permite a criação da sala de guerra remota (Acampa Meet) e a ferramenta de análise de ameaças (Mal Where).

Já a terceira fase aborda um vazamento de dados, onde são exfiltrados dados pessoais controlados pela empresa petrolífera. O desafio exige que o jogador valide da legitimidade do incidente, identifique a natureza dos dados vazados, determine a necessidade de comunicações públicas, sinalize a causa raiz e auxilie na desativação da infraestrutura do grupo atacante. Para complementar a narrativa, foram criadas ferramentas que permitem a inspeção de pacotes e sites que decodificam dados e simulam a aplicação real “whois”. A Figura 1 ilustra um exemplo de tomada de decisão apresentada na aplicação Acampa Meet (A), bem como as interfaces das ferramentas ANEXUS Mail (B), Remotenik (C) e Tick Task (D).

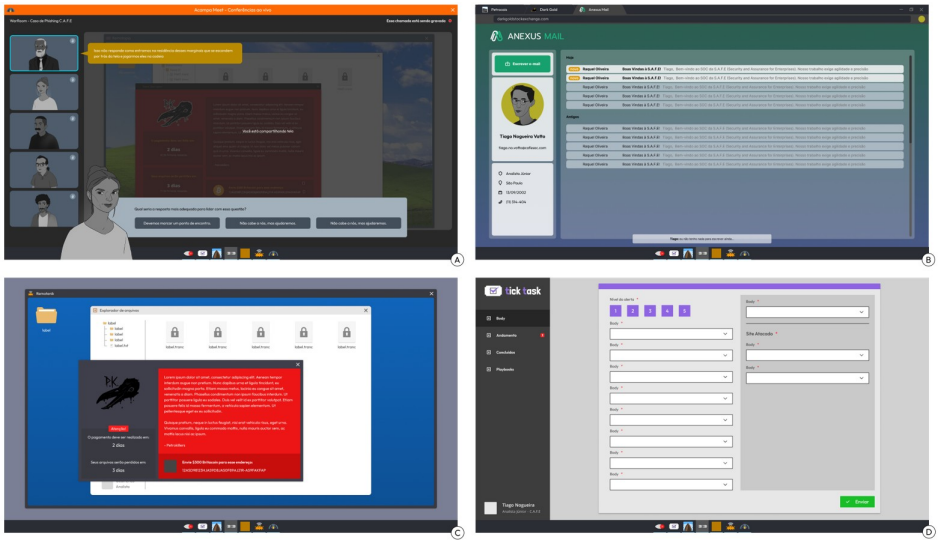

Figura 1. Imagens das aplicações Acampa Meet (A), ANEXUS Mail (B), Remotenik (C) e Tick Task (D).

O desempenho do jogador é quantificado com base na precisão de suas decisões e refletido na variação da cotação das ações da PetroCAIS na bolsa de valores fictícia Gold Dark Exchange. O sistema de pontuação é apresentado em tempo real por meio de *pop-ups*

de aviso, que notificam o jogador sobre os acertos e equívocos de suas escolhas, impactando diretamente o valor dos ativos da organização no mercado financeiro. Esse mecanismo de *feedback* constante simula a pressão corporativa e a responsabilidade atrelada à gestão de incidentes em ambientes reais de SOC.

A experiência de jogo é enriquecida por elementos narrativos que asseguram a imersão do jogador. A introdução ocorre por meio de uma *cutscene* inicial que estabelece a ambientação da trama, enquanto *cutscenes* intermediárias garantem a transição narrativa entre os papéis técnicos e o avanço pelas fases. Ao final da jornada, sequências específicas de vitória ou *game over* concluem o ciclo da narrativa. A Figura 2 apresenta um trecho da *cutscene* inicial, utilizada para introduzir a narrativa do jogo, a partir da sequência de imagens estáticas de personagens e textos.

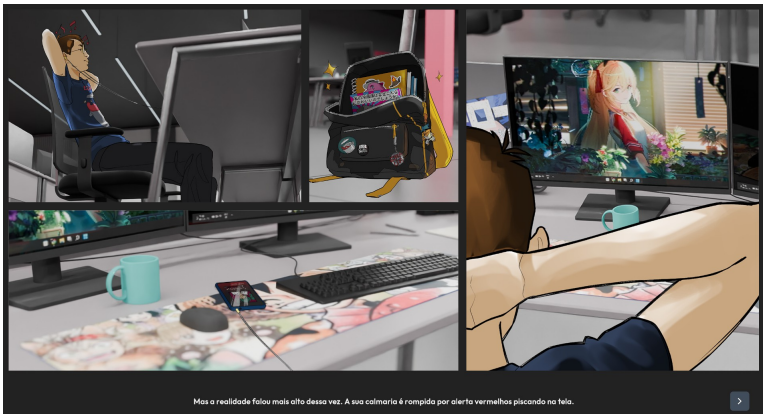

Figura 2. Trecho da *cutscene* inicial do jogo.

Quanto aos seus aspectos funcionais, o jogo implementa persistência de dados para assegurar a continuidade da experiência do jogador entre sessões distintas. O jogo registra *checkpoints* a cada transição de personagem, permitindo que um jogador opte entre retomar o progresso no último ponto registrado ou iniciar uma nova sessão, garantindo a preservação do histórico de aprendizado. Para consolidar o aprendizado sobre resposta a incidentes cibernéticos, o jogo integra ao final de cada fase um módulo educacional composto por aulas técnicas que aprofundam os conceitos vivenciados na simulação. Para a transmissão desse conteúdo, adotou-se o gênero *Visual Novel*, uma técnica de narrativa japonesa que utiliza imagens estáticas e diálogos textuais (Camingue; Carstensdottir; Melcer, 2021). Essa escolha permitiu uma transição entre a leitura de tópicos técnicos e a interação com os diálogos dos personagens do jogo.

Durante a execução das aulas, o conteúdo é mediado por slides técnicos, que servem como guia visual e referência teórica para a narrativa. A exposição é conduzida por três personagens selecionados para cada fase, que interagem entre si em um formato de painel instrutivo. Para conferir dinamismo, o sistema aplica um efeito de foco seletivo; conforme o diálogo avança na parte inferior da tela, o personagem ativo ganha destaque visual, enquanto os demais permanecem em um estado de opacidade, sinalizando a alternância das falas. A Figura 3 ilustra a interface de uma das aulas, exibindo a sala do SOC, o slide técnico de referência, a disposição dos três personagens e a caixa de diálogos ativa.

Por fim, considerando que cada módulo de aula possui aproximadamente 35 minutos de conteúdo, buscou-se mitigar o risco de fadiga do jogador. Para garantir que

Figura 3. Interface criada para a apresentação das aulas do jogo.

o jogador se mantenha engajado, foi implementada uma funcionalidade que permite ao participante escolher entre a visualização do conteúdo na íntegra (focada na imersão técnica) ou acessar uma versão resumida (focada nos conceitos essenciais de cada tópico). Essa estratégia garante que o elemento educacional seja preservado, ao mesmo tempo em que se respeita a disponibilidade de tempo e o conhecimento prévio de cada jogador.

4. Avaliação do Jogo Educacional

Os autores conduziram avaliações relacionadas à experiência de diferentes públicos em relação ao We Got Hacked!. Uma primeira análise da experiência de estudantes universitários concentrou-se na primeira fase do jogo (Steigleder et al., 2025). Dando continuidade a esse processo, este trabalho detalha a segunda avaliação, realizada em janeiro de 2026, que focou na percepção de usuários sobre a usabilidade da solução, utilizando a versão do jogo lançada em dezembro de 2025.

A amostra foi composta por 29 residentes convidados pelo Programa Hackers do Bem da RNP. Deste total, 25 residentes concluíram integralmente a avaliação (taxa de conclusão de 86,2%). Os participantes foram divididos em duas turmas e submetidos a um protocolo de duas etapas que envolvia (1) a execução da versão completa do We Got Hacked! e (2) o pós-teste de experiência, com foco na mensuração da usabilidade e na identificação de oportunidades de aprimoramento nas mecânicas de jogo.

As duas etapas foram conduzidas de forma remota assíncrona e em ambiente não controlado. As atividades seguiram um cronograma pré-estabelecido, com o suporte sob demanda dos autores via aplicativo de mensagens. Como subsídio teórico e operacional foram disponibilizados antecipadamente dois materiais audiovisuais: um vídeo detalhando o projeto do jogo e outro com orientações sobre as atividades, cronograma e o preenchimento dos instrumentos de coleta.

A coleta de dados foi realizada via plataforma Microsoft Forms, a partir de questões baseadas no MEEGA+, um modelo de avaliação de jogos educacionais proposto por Petri, Wangenheim e Borgatto (2019). O questionário original do modelo foi adaptado para 25 questões, distribuídas em sete dimensões (Usabilidade, Confiança, Desafio, Satisfação, Diversão, Atenção focada e Relevância do jogo). O instrumento utiliza uma escala Likert de 5 pontos, variando de “discordo totalmente” (-2) a “concordo totalmente” (+2).

Para complementar as métricas quantitativas do modelo MEEGA+, também foram coletadas as impressões subjetivas dos participantes. A partir de dois campos abertos, os residentes detalharam as características interessantes do jogo (pontos fortes da experiência) e apresentaram sugestões de melhorias (oportunidades de aprimoramento). Além disso, para permitir a análise cruzada dos resultados, a avaliação de experiência incluiu a coleta de informações demográficas e de perfil dos participantes.

Após o encerramento da coleta, os dados brutos foram tratados e categorizados pelos autores. As respostas do modelo MEEGA+ foram transpostas para a sua matriz analítica, permitindo o cálculo automatizado de médias, medianas e conceitos de desempenho para as dimensões avaliadas. Paralelamente, os dados demográficos e de perfil dos residentes foram organizados em uma base independente para a correlação. Quanto aos dados qualitativos dos campos abertos, aplicou-se uma análise de conteúdo para categorizar as sugestões de melhoria e os pontos positivos destacados pelos residentes.

5. Resultados

A análise quantitativa revelou uma percepção majoritariamente positiva do We Got Hacked!. As maiores médias foram registradas na dimensão de Relevância, com destaque para a percepção de valor do conteúdo e a adequação do jogo como método de ensino. Esses dados, somados aos altos índices das dimensões Diversão e Satisfação podem indicar que o jogo obteve sucesso em sua proposta de ser um recurso educacional engajador, além de sugerir que está alinhado aos interesses profissionais dos residentes. A estética do jogo também foi validada positivamente, conforme apontou o resultado das questões que avaliavam o seu visual.

Em contrapartida, as menores médias revelaram pontos para a evolução do jogo. A dimensão de Atenção Focada apresentou o resultado mais baixo, situando-se na zona de neutralidade. O resultado pode sugerir que embora o jogo seja relevante, o nível de imersão ainda pode ser otimizado. Outro ponto sensível foi a dificuldade de recuperação após erros dos jogadores. Esse dado pode correlacionar-se com o *feedback* sobre a ausência de um sistema de salvamento de progresso da versão, reforçando que a punição por erro (ter que reiniciar o jogo) pode ter impactado na percepção da usabilidade técnica.

A análise agregada das dimensões, ilustrada no gráfico radar da Figura 4, sintetiza o equilíbrio do simulador. Enquanto dimensões como Relevância (média 1,53) e Diversão (média 1,38) atingiram conceitos sólidos de “Concordo”, a Usabilidade (média 0,68) e a Atenção Focada (média 0,21) permaneceram na zona de “Nem concordo, nem discordo”. Esse diagnóstico sugere que o jogo possui base educacional e narrativa adequadas, mas demanda refinamentos na mecânica de suporte ao erro e em elementos imersivos para potencializar a experiência do usuário.

A avaliação da experiência dos residentes com o We Got Hacked! foi aprofundada por meio de uma análise qualitativa das respostas dos campos abertos. Os relatos espontâneos permitiram identificar como os usuários perceberam a fluidez, a narrativa e os desafios técnicos da plataforma. Esta etapa foi importante para validar o realismo do jogo e elencar prioridades técnicas para as próximas versões. Os *feedbacks* positivos podem sugerir que o jogo cumpre os objetivos principais de engajamento e fidelidade técnica, considerando a quantidade de menções positivas para “mecânica e diversão” (20 menções), “fidelidade e realismo” (19 menções), “narrativa e estética” (16 menções) e

Médias da avaliação por dimensão	
Dimensão	Média
Usabilidade	0,68
Confiança	0,88
Desafio	0,84
Satisfação	1,18
Diversão	1,38
Atenção Focada	0,21
Relevância	1,53

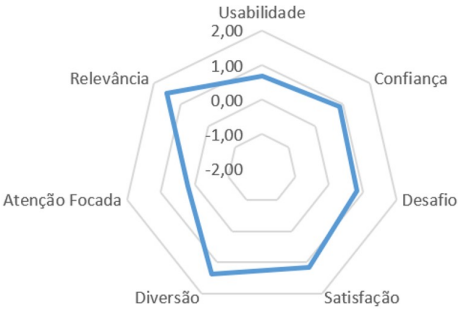

Figura 4. Tabela e gráfico radar das médias por dimensão.

"eficácia educacional" (7 menções).

Entretanto, as sugestões de melhorias indicaram direções para a evolução do jogo. A necessidade de salvamento do progresso (11 menções) e um mecanismo de validação do cadastro e recuperação de senhas (2 menções), indicou a necessidade de alteração da estrutura da aplicação. Adicionalmente, houve solicitação por melhores alertas sobre erros cometidos durante o jogo (13 menções), especialmente em relação à oscilação do "preço da ação" (indicador de desempenho no jogo) e por *feedbacks* mais detalhados ao final de cada fase.

6. Conclusão

Este artigo sintetizou o ciclo de desenvolvimento do projeto We Got Hacked!, jogo educacional voltado à capacitação em resposta a incidentes cibernéticos que simula o ambiente operacional e o fluxo de trabalho de um SOC. O resultado da avaliação externa realizada com os residentes do Programa Hackers do Bem indicou a percepção do We Got Hacked! como uma ferramenta divertida e relevante para o aprendizado de segurança cibernética.

Uma limitação do estudo está relacionada com a natureza assíncrona das etapas em ambiente remoto, resultando na realização de uma avaliação em um ambiente não controlado. Em função disso, não foi possível descartar a influência de variáveis externas em relação ao engajamento dos participantes e ao compartilhamento de informações durante o preenchimento dos questionários. Esta limitação serve como base para trabalhos futuros, os quais poderão empregar uma abordagem para mensurar, em ambiente controlado, o ganho e a retenção do aprendizado promovidos pela versão mais atualizada de We Got Hacked!. Além disso, a avaliação dos residentes indicou oportunidades para futuras expansões do jogo, incluindo a implementação de módulos colaborativos e competitivos, módulos educacionais e a portabilidade do jogo para dispositivos móveis. Novos estudos poderão avaliar o impacto da implementação das expansões sugeridas na experiência e no aprendizado dos jogadores.

Agradecimentos

O presente trabalho foi realizado com o apoio do Programa Hackers do Bem no Domínio Cibernético, executado pela RNP e SENAI, coordenado pela Softex e financiado pelo MCTI com recursos oriundos da Lei das TICs – Lei nº 8.248, de 23 de outubro de 1991.

Referências

ANGAFOR, G.; YEVSEYEVA, I.; MAGLARAS, L. MalAware: A tabletop exercise for malware security awareness education and incident response training. *Internet of Things and Cyber-Physical Systems*, Elsevier, 2024.

ANGAFOR, G. N.; YEVSEYEVA, I.; MAGLARAS, L. Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, Emerald Publishing Limited, v. 31, n. 4, 2023.

CAMINGUE, J.; CARSTENSDOTTIR, E.; MELCER, E. F. What is a visual novel? *Proceedings of the ACM on Human-Computer Interaction*, ACM New York, NY, USA, v. 5, n. CHI PLAY, p. 1–18, 2021.

CHECK POINT. *Global Cyber Attacks Rise in January 2026 Amid Increasing Ransomware Activity and Expanding GenAI Risks*. 2026. Acesso em 14-jul-2026. Disponível em: ⟨https://blog.checkpoint.com/research/global-cyber-attacks-rise-in-january-2026-amid-increasing-ransomware-activity-and-expanding-genai-risks/⟩.

HATZIVASILIS, G. et al. The threat-arrest cyber range platform. In: IEEE. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. [S.l.], 2021.

IBM. *Cost of a Data Breach Report 2025*. 2025. Acesso em 13-jul-2026. Disponível em: ⟨https://www.ibm.com/reports/data-breach⟩.

ISACA. *State of Cybersecurity 2023 report*. 2023. Acesso em 30-jun-2025. Disponível em: ⟨https://www.isaca.org/resources/reports/state-of-cybersecurity-2023⟩.

KATSANTONIS, M. N.; MAVRIDIS, I.; GRITZALIS, D. Design and evaluation of cofelet-based approaches for cyber security learning and training. *Computers & Security*, Elsevier, v. 105, 2021.

KHANDO, K. et al. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, v. 106, 2021.

KITCHENHAM, B. A.; BUDGEN, D.; BRERETON, P. *Evidence-based software engineering and systematic reviews*. [S.l.]: CRC press, 2015. v. 4.

O'CONNOR, S. et al. SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security. *Information Sciences*, Elsevier, v. 580, 2021.

PÉREZ, J.; CASTRO, M.; LÓPEZ, G. Serious games and AI: Challenges and opportunities for computational social science. *IEEE Access*, IEEE, v. 11, 2023.

PETRI, G.; WANGENHEIM, C. G. V.; BORGATTO, A. F. MEEGA+: Um modelo para a avaliação de jogos educacionais para o ensino de computação. *Revista Brasileira de Informática na Educação*, v. 27, 2019.

PIRTA-DREIMANE, R. et al. Try to esCAPE from cybersecurity incidents! A technology-enhanced educational approach. *Technology, Knowledge and Learning*, Springer, 2024.

STEIGLEDER, R. et al. Análise da percepção de estudantes sobre um jogo educacional de resposta a incidentes cibernéticos. In: SBC. *Escola Regional de Redes de Computadores (ERRC)*. [S.l.], 2025. p. 95–101.

THAROT, K. et al. A cybersecurity training concept for cyber-physical manufacturing systems. *Procedia CIRP*, Elsevier, v. 120, 2023.

VIDENOVIK, M.; FILIPOSKA, S.; TRAJKOVIK, V. A novel methodological approach for learning cybersecurity topics in primary schools. *Multimedia Tools and Applications*, Springer, 2024.