Análise da percepção de estudantes sobre um jogo educacional de resposta a incidentes cibernéticos

Rodrigo Steigleder[1], Luciano Ignaczak[1], Mauricio Bammann Gehling[1], Bernardo Klein[1], Igor Flores[1], Jairo Augusto de Campos Alff[1], Tiago Umberto Gazzola[1]

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

steigleder@outook.com, {lignaczak,mgehling}@unisinos.br,

{bernardoklein,igorflores,jairoalff,tiagoug}@edu.unisinos.br

Abstract. *The increase in cyber incidents underscores the need for incident response training. However, the literature indicates a gap in Portuguese-language digital games that simulate the daily routine of incident response teams. This study evaluates the first phase of We Got Hacked!, a simulation game for cyber incident response training, by administering a post-test questionnaire to 15 university students. The results indicated high scores in the relevance and usability categories; however, they suggest increasing the difficulty of the game's challenges.*

Resumo. *O aumento dos incidentes cibernéticos destaca a necessidade de treinamento em resposta a incidentes. Contudo, a literatura indica uma lacuna em relação a jogos digitais em língua portuguesa que simulam o cotidiano de times de resposta a incidentes. Este estudo avalia a primeira fase de We Got Hacked!, um jogo de simulação para capacitação em resposta a incidentes cibernéticos, aplicando um questionário pós-teste em 15 estudantes de graduação. Os resultados indicaram altas pontuações em categorias de relevância e usabilidade; contudo, sugerem a necessidade de aumentar a dificuldade dos desafios do jogo.*

1. Introdução

As organizações estão expostas ao risco de ataques cibernéticos e é desejável que elas respondam rapidamente com o objetivo de conter um incidente ou limitar suas consequências. Para isso, elas mantêm times de resposta a incidentes de segurança da informação (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].

No cenário atual, incidentes de segurança cibernética causam impactos significativos às organizações [Nelson et al. 2024]. A complexidade destes incidentes pode ser acentuada pela inexperiência dos profissionais dos times de segurança. Atualmente,

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

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

44% das equipes de segurança são compostas por membros com menos de três anos experiência [ISACA 2023]. Diante deste cenário, jogos educacionais surgem como uma opção eficiente para treinamento em segurança cibernética [Khando et al. 2021], demonstrando potencial pedagógico ao proporcionar um ambiente para o aprendizado e o desenvolvimento da autoconfiança dos usuários [Pérez et al. 2023, Angafor et al. 2024, Pirta-Dreimane et al. 2024].

Apesar dos avanços em jogos educacionais, a literatura indica uma lacuna significativa, devido, principalmente, à inexistência de jogos com conteúdo em língua portuguesa. Além disso, há uma quantidade reduzida de publicações focadas em soluções digitais que simulam respostas a incidentes. O presente estudo pretende preencher esta lacuna, analisando o contexto de estudantes para responder a questão de pesquisa "como os jogadores percebem a experiência de um jogo de simulação de resposta a incidentes de segurança cibernética?". Para isso, este trabalho avalia a primeira fase de We Got Hacked!, um jogo educacional desenvolvido em português que busca capacitar profissionais e estudantes para atuação em times de resposta a incidentes. O objetivo é mensurar a experiência utilizando um questionário que combinou a análise de dados demográficos e o modelo MEEGA+.

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 a primeira fase do jogo desenvolvido. A Seção 4 documenta a metodologia utilizada para a primeira avaliação externa do jogo. Na seção 5 são discutidos os resultados obtidos na pesquisa. Por fim, a Seção 6 apresenta as conclusões, futuras pesquisas e limitações deste estudo.

2. Trabalhos Relacionados

A fase de pesquisa foi iniciada em janeiro de 2025, aplicando uma metodologia de revisão sistemática baseada no *framework* de [Kitchenham et al. 2015]. Para a obtenção dos trabalhos, foram selecionadas as bases de dados científicas Emerald[3], IEEE Xplore[4], Science Direct[5], Springer[6], Taylor & Francis[7] e Wiley[8]. A pesquisa considerou artigos publicados a partir de 2020 e utilizou uma *string* de busca que concatenou palavras-chave de 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*). Inicialmente, 62 publicações foram retornadas e, após rodadas de avaliação e eliminação, oito artigos foram selecionados para análise final.

A avaliação da literatura demonstrou o impacto positivo na utilização 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 a conscientização sobre a postura corporativa em relação a riscos cibernéticos [Angafor et al. 2024, Angafor et al. 2023]. De forma complementar, o trabalho de

[3]https://www.emerald.com/insight/
[4]https://ieeexplore.ieee.org/Xplore/home.jsp
[5]https://www.sciencedirect.com/
[6]https://link.springer.com/
[7]https://www.tandfonline.com/
[8]https://onlinelibrary.wiley.com/

[Pirta-Dreimane et al. 2024] implementou um jogo baseado em *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 esses treinamentos customizáveis preparam os participantes para mitigar incidentes em condições reais.

Estudos também apresentaram a implementação e a avaliação de jogos de segurança ofensiva e de tomada de decisão em resposta a incidentes [Katsantonis et al. 2021, O'Connor et al. 2021]. Além disso, o artigo de [Videnovik et al. 2024] indicou o sucesso no ensino de fundamentos de segurança a alunos de ensino primário a partir da aplicação de jogos educacionais em sala de aula . Por fim, a pesquisa de [Tharot et al. 2023] apontou a necessidade da investigação da sequência pedagógica do conteúdo de jogos de segurança cibernética para profissionais da área industrial.

A literatura indica uma predominância de jogos educacionais voltados para a simulação de ataques cibernéticos e para o treinamento em conscientização sobre o tema. Em relação a área de resposta a incidentes, os jogos indicados restringem-se a formatos como *tabletop*, jogos físicos ou exercícios remotos. A única exceção digital, o jogo baseado em cenários apresentado no trabalho de [O'Connor et al. 2021], foca na tomada de decisão, mas não simula o fluxo de trabalho do time de resposta a incidentes de um SOC. 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 de simulação no formato *single-player*, em língua portuguesa e disponível como aplicação *web*. O jogo, desenvolvido usando Unity, foi projetado para capacitar estudantes e profissionais em resposta a incidentes cibernéticos, sendo inspirado na rotina de um SOC. Seu principal objetivo é desenvolver o raciocínio crítico e a agilidade na tomada de decisões em um ambiente de simulação realista. Detalhes sobre o desenvolvimento do jogo, incluindo capturas de tela e explicações adicionais, foram compartilhados na *landing page* do projeto[9].

O contexto do jogo apresenta o conflito entre uma organização petrolífera e um grupo hacktivista. O jogador assume diversos papéis do time de resposta a incidentes de uma empresa especializada em segurança cibernética, contratada pela organização petrolífera, sendo encarregado de reagir aos incidentes e defender os sistemas desta organização. A narrativa foi projetada para se desenvolver em três fases, simulando cenários reais de incidentes de pichação de site (*defacement*), ataques de *ransomware* e vazamentos de dados.

A primeira fase do jogo simula um ataque de *defacement* ao site da organização petrolífera. Esse foi o incidente disponibilizado à amostra de estudantes e constitui o objeto deste estudo. Para resolvê-lo, o jogador assume, inicialmente, o papel do analista N1 do SOC, sendo apresentado à tela que simula uma área de trabalho com diversas funções. O primeiro objetivo é determinar a legitimidade da ameaça através da investigação visual

[9]https://github.com/AtomicRocketEntertainment/We-Got-Hacked

do site. Após a confirmação, o jogador deve analisar alertas em um SIEM e criar um *ticket* no sistema de gestão. Posteriormente, assumindo a função da coordenadora do SOC, o jogador é responsável pela comunicação formal do incidente com o personagem técnico da petrolífera.

Em seguida, a responsabilidade é repassada para o analista N2 do SOC, que assume as atividades de contenção e recuperação do incidente. Essas ações incluem a retirada do site afetado do ar, a investigação das vulnerabilidades do serviço atacado, a identificação da correção necessária, a restauração do *backup* do site e, por fim, o restabelecimento do serviço. Para executar esses passos, o jogador é guiado por um *playbook* e pela troca de mensagens entre os personagens. O desempenho do jogador é avaliado pelo número de decisões corretas e incorretas tomadas, cujo impacto se reflete no preço de mercado da empresa petrolífera.

4. Metodologia

Com o objetivo de avaliar a primeira fase de We Got Hacked! e obter evidências das contribuições do jogo, foi conduzida uma avaliação externa em agosto de 2025. O estudo envolveu a aplicação de um questionário para avaliar questões como a experiência, a diversão e a usabilidade do jogo. A amostra contou com a participação virtual de 15 estudantes da graduação em Segurança da Informação da UNISINOS, que foram convidados pela coordenação do curso. O questionário para a coleta de dados foi hospedado em um formulário virtual criado com a ferramenta gratuita Microsoft Forms[10].

Após a finalização da coleta, os dados do questionário foram armazenados e, posteriormente, transferidos para uma planilha Excel para análise. O perfil da amostra foi composto integralmente por estudantes na faixa etária de 20 a 29 anos, sendo 93% dela do gênero masculino. Em relação à experiência profissional, mais da metade dos estudantes (53%) ainda não atua na área, dois participantes (14%) possuem menos de um ano de experiência e um terço (33%) possui entre um e três anos de experiência em segurança cibernética.

Para avaliar a experiência dos avaliadores com o *gameplay*, foi utilizado um questionário baseado no MEEGA+, um modelo de avaliação de jogos educacionais [Petri et al. 2019]. O questionário original do modelo foi adaptado pelos pesquisadores para 25 questões, distribuídas em sete dimensões que avaliam: usabilidade, confiança, desafio, satisfação, diversão, atenção focada e relevância do jogo. Os avaliadores classificaram as questões utilizando uma escala Likert de 5 pontos, variando de "discordo totalmente" (-2) a "concordo totalmente" (+2).

5. Resultados

O resultado da avaliação quantitativa das 25 questões do modelo MEEGA+, apresentado na Figura 1, revelou uma percepção positiva da primeira fase do We Got Hacked!. A grande maioria das questões obteve conceitos elevados (onze com "concordo plenamente" e dez com "concordo"), com pouca discordância geral. Os participantes confirmaram a experiência lúdica positiva e a relevância pedagógica, com altas médias em diversão (Q17), recomendação (Q16), mecânica (Q3) e relação com a disciplina (Q23). Contudo, a análise do desafio do jogo (Q11) foi moderada.

[10]https://forms.office.com/r/xZLsh3wwPh

Dimensão	#	Questões	Média	Mediana	Conceito
Usabilidade	Q1	O design do jogo é atraente	0,53	1	Concordo
	Q2	Eu precisei aprender poucas coisas para poder começar a jogor o jogo	1,40	2	Concordo plenamente
	Q3	Aprender a jogar este jogo foi fácil para mim	1,80	2	Concordo plenamente
	Q4	Eu acho que a maioria das pessoas aprenderiam a jogar este jogo rapidamente	1,00	1	Concordo
	Q5	Eu considero que o jogo é fácil de jogar	1,33	1	Concordo
	Q6	As regras do jogo são claras e compreensíveis	1,40	2	Concordo plenamente
	Q7	As cores utilizadas no jogo são compreensíveis	1,33	2	Concordo plenamente
	Q8	Quando eu cometo um erro é fácil de me recuperar rapidamente	1,33	2	Concordo plenamente
Confiança	Q9	Quando olhei pela primeira vez o jogo, eu tive a impressão de que seria fácil para mim	1,27	1	Concordo
	Q10	A organização do conteúdo me ajudou a estar confiante de que eu iria aprender com este jogo	1,13	1	Concordo
Desafio	Q11	Este jogo é adequadamente desafiador para mim	- 0,40	0	Nem concordo, nem discordo
	Q12	O jogo não se torna monótono na suas tarefas (repetitivo ou com tarefas chatas)	0,67	1	Concordo
Satisfação	Q13	Completar as tarefas do jogo me deu um sentimento de realização	1,27	1	Concordo
	Q14	É devido ao meu esforço pessoal que eu consigo avançar no jogo	1,13	1	Concordo
	Q15	Me sinto satisfeito com as coisas que aprendi no jogo	1,27	2	Concordo plenamente
	Q16	Eu recomendaria este jogo para meus colegas	1,60	2	Concordo plenamente
Diversão	Q17	Eu me diverti no jogo	1,47	2	Concordo plenamente
	Q18	Aconteceu alguma situação durante o jogo (elementos do jogo, competição, etc) que me fez sorrir	0,93	1	Concordo
Atenção focada	Q19	Houve algo interessante no início do jogo que capturou minha atenção	0,20	0	Nem concordo, nem discordo
	Q20	Eu estava tão envolvido no jogo que eu perdi noção do tempo	0,20	0	Nem concordo, nem discordo
	Q21	Eu esqueci sobre o ambiente ao meu redor enquanto jogava este jogo	0,07	0	Nem concordo, nem discordo
Relevância	Q22	O conteúdo do jogo é relevante para os meus interesses	1,60	2	Concordo plenamente
	Q23	É claro para mim como o conteúdo do jogo está relacionado com a disciplina	1,73	2	Concordo plenamente
	Q24	O jogo é um método de ensino adequado para esta disciplina	1,53	2	Concordo plenamente
	Q25	Eu prefiro aprender com este jogo do que de outra forma (outro método de ensino)	0,73	1	Concordo

Figura 1. Resultados das questões que mensuram a experiência dos avaliadores.

Para obter uma visão sintética da avaliação, os resultados das 25 questões foram agrupados por suas respectivas dimensões, considerando as médias obtidas para cada categoria. A Figura 2 apresenta a tabela com as médias para cada dimensão, além da representação em um gráfico radar. A análise por dimensão indica que as maiores pontuações foram concentradas em "usabilidade" , "satisfação", "diversão", "confiança" e "relevância", indicando que a primeira fase de We Got Hacked! foi percebida de forma positiva pelos estudantes, confirmando o potencial do jogo. Enquanto as menores pontuações foram observadas nas dimensões de "desafio" e "atenção focada", indicando novamente a necessidade de aprimoramento no desenvolvimento do projeto.

Médias da avaliação por dimensão	
Dimensão	Média
Usabilidade	1,27
Confiança	1,20
Desafio	0,13
Satisfação	1,32
Diversão	1,20
Atenção Focada	0,16
Relevância	1,40

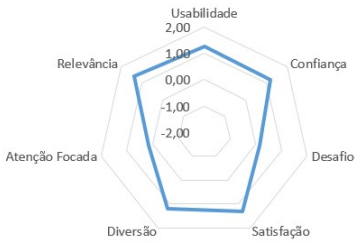

Figura 2. Médias de avaliação por dimensão e a representação em gráfico radar.

Para aprofundar a compreensão dos resultados, a avaliação das dimensões foi cruzada com o perfil profissional dos participantes. Para isso, compararam-se as avaliações dos alunos que não atuam na área ou que possuem no máximo um ano de experiência (grupo A) com aqueles que possuem entre um e três anos de experiência na área de segurança cibernética (grupo B). De maneira geral, a análise por perfil, apresentada na Figura 3, revela uma inversão na percepção da experiência do jogo. O grupo A (menos experiente) avaliou a experiência como mais divertida, satisfatória e relevante (1,40, 1,35 e 1,58, respectivamente).

Em contraste, o grupo B (mais experiente) atribuiu notas mais altas para a "usabilidade" (1,43), percebendo o jogo como menos divertido e satisfatório (0,80 e 1,25, respectivamente). Essa disparidade pode sugerir que a percepção do jogo é influenciada pela

Médias da avaliação por dimensão e perfil		
Dimensão	**Grupo A (menos experiente)**	**Grupo B (mais experiente)**
Usabilidade	1,19	1,43
Confiança	1,25	1,10
Desafio	0,00	0,40
Satisfação	1,35	1,25
Diversão	1,40	0,80
Atenção Focada	0,10	0,27
Relevância	1,58	1,05

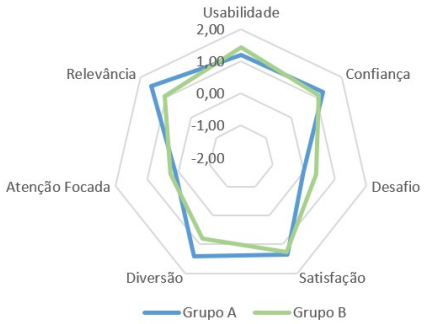

Figura 3. Médias por perfil e a representação em gráfico radar.

base de conhecimento pré-existente do jogador. Apesar de os profissionais com mais experiência tenham validado a usabilidade do jogo, eles parecem demandar um nível maior de desafio e complexidade para que a experiência seja considerada igualmente lúdica e relevante.

Embora esperasse que a fase introdutória de um jogo apresentasse baixo nível de dificuldade, as pontuações na dimensão de "desafio" indicam a necessidade de aumentar a sua complexidade. Em resposta a essa demanda, as duas fases subsequentes foram aprimoradas (as quais não foram alvo desta avaliação). Para aprofundar a investigação, foram incluídas ferramentas que permitem a inspeção de pacotes de rede, a avaliação de assinaturas de ameaças e a identificação de endereços externos maliciosos. Além disso, o jogador auxilia na gestão de crise, participando de uma sala de guerra ativada em resposta aos ataques de *ransomware* e vazamento de dados.

6. Conclusão

Este estudo avaliou a primeira fase do We Got Hacked! por meio de um questionário aplicado a estudantes de graduação em Segurança da Informação, utilizando o modelo MEEGA+. A avaliação foi majoritariamente positiva, indicando que o jogo é uma ferramenta de aprendizado útil e com alta relevância para a área de atuação, especialmente nos quesitos de usabilidade. Essa contribuição é significativa, considerando a carência de jogos digitais que simulam o cotidiano de times de resposta a incidentes cibernéticos e que possuem conteúdo em língua portuguesa. Contudo, a análise também sugere a necessidade de aprimoramentos no nível de desafio do simulador.

A pesquisa apresenta limitações, notadamente em relação ao tamanho reduzido da amostra, que impede a generalização dos resultados, e a metodologia, que limita a mensuração do ganho de aprendizado. Estas limitações servem de base para trabalhos futuros. Com a finalização completa do jogo, um trabalho futuro usará uma abordagem para mensurar o aprendizado percebido a partir da experiência promovida pelo We Got Hacked!.

Agradecimentos

O presente trabalho foi realizado com o apoio do Programa Hackers do Bem no Domínio Cibernético, financiado pelo MCTI com recursos oriundos da Lei das TICs - Lei nº 8.248, de 23 de outubro de 1991, no âmbito do PPISOFTEX, coordenado pela Softex e publicado PDI 03, DOU 01245.023862/2022-14.

Referências

Angafor, G., Yevseyeva, I., and Maglaras, L. (2024). MalAware: A tabletop exercise for malware security awareness education and incident response training. *Internet of Things and Cyber-Physical Systems*.

Angafor, G. N., Yevseyeva, I., and Maglaras, L. (2023). Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*, 31(4).

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T., et al. (2021). The threat-arrest cyber range platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE.

ISACA (2023). State of Cybersecurity 2023 report. `https://www.isaca.org/resources/reports/state-of-cybersecurity-2023`. Acesso em 30-jun-2025.

Katsantonis, M. N., Mavridis, I., and Gritzalis, D. (2021). Design and evaluation of cofelet-based approaches for cyber security learning and training. *Computers & Security*, 105.

Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106.

Kitchenham, B. A., Budgen, D., and Brereton, P. (2015). *Evidence-based software engineering and systematic reviews*, volume 4. CRC press.

Nelson, A., Rekhi, S., Souppaya, M., and Scarfone, K. (2024). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile. Technical report, National Institute of Standards and Technology.

O'Connor, S., Hasshu, S., Bielby, J., Colreavy-Donnelly, S., Kuhn, S., Caraffini, F., and Smith, R. (2021). SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security. *Information Sciences*, 580.

Pérez, J., Castro, M., and López, G. (2023). Serious games and AI: Challenges and opportunities for computational social science. *IEEE Access*, 11.

Petri, G., Von Wangenheim, C. G., and Borgatto, A. F. (2019). MEEGA+: Um modelo para a avaliação de jogos educacionais para o ensino de computação. *Revista Brasileira de Informática na Educação*, 27.

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., and Bonders, M. (2024). Try to esCAPE from cybersecurity incidents! A technology-enhanced educational approach. *Technology, Knowledge and Learning*.

Tharot, K., Duong, Q. B., Riel, A., and Thiriet, J.-M. (2023). A cybersecurity training concept for cyber-physical manufacturing systems. *Procedia CIRP*, 120.

Videnovik, M., Filiposka, S., and Trajkovik, V. (2024). A novel methodological approach for learning cybersecurity topics in primary schools. *Multimedia Tools and Applications*.