EDUCAÇÃO HACKER E GAMIFICAÇÃO COM RPG MAKER: METODOLOGIAS ATIVAS NA FORMAÇÃO CRÍTICA EM CIBERSEGURANÇA

HACKER EDUCATION AND GAMIFICATION WITH RPG MAKER: ACTIVE METHODOLOGIES IN CRITICAL CYBERSECURITY TRAINING

Tadeu Marcos Borges Paes[1]

Murilo Ruan Silva Matos[2]

Resumo: A educação hacker propõe uma pedagogia baseada na curiosidade, na ética e na experimentação. Ao ser associada à gamificação, ela ganha um novo espaço de expressão criativa, capaz de transformar o aprendizado em cibersegurança em uma experiência interativa e significativa. Este artigo analisa a utilização do RPG Maker como ferramenta de gamificação e metodologia ativa na Educação Hacker, explorando seu potencial para desenvolver competências investigativas, éticas e colaborativas. A partir de uma abordagem teórico-reflexiva, discutem-se os fundamentos da aprendizagem baseada em desafios e os princípios do design de jogos como práticas formativas que estimulam o pensamento crítico e a resolução de problemas reais em contextos de segurança digital. O uso do RPG Maker, além de aproximar o estudante da lógica da programação e da simulação de incidentes cibernéticos, possibilita a criação de narrativas educativas que despertam empatia, tomada de decisão e senso de responsabilidade ética. Assim, a gamificação emerge como linguagem e estratégia de emancipação cognitiva no processo de formação hacker.

1 Doutorando em Inteligência Artificial pela Senai Centro Desenvolvimento da Amazônia, Orcid: https://orcid.org/0009-0002-2978-2117

2 Discente de Licenciatura Plena em Computação pela UFRA - Universidade Federal Rural da Amazônia, Orcid: https://orcid.org/0009-0005-5734-3324

Palavras-chave: Educação hacker. Gamificação. RPG Maker. Metodologias ativas. Cibersegurança.

Abstract: Hacker education proposes a pedagogy based on curiosity, ethics, and experimentation. When associated with gamification, it gains a new space for creative expression, capable of transforming cybersecurity learning into an interactive and meaningful experience. This article analyzes the use of RPG Maker as a gamification tool and active methodology in Hacker Education, exploring its potential to develop investigative, ethical, and collaborative skills. From a theoretical-reflective approach, the fundamentals of challenge-based learning and the principles of game design are discussed as formative practices that stimulate critical thinking and the resolution of real-world problems in digital security contexts. The use of RPG Maker, in addition to bringing students closer to the logic of programming and the simulation of cyber incidents, enables the creation of educational narratives that awaken empathy, decision-making, and a sense of ethical responsibility. Thus, gamification emerges as a language and strategy for cognitive emancipation in the hacker training process.

Keywords: Hacker education. Gamification. RPG Maker. Active methodologies. Cybersecurity.

INTRODUÇÃO

A crescente digitalização da sociedade transformou o ciberespaço em um ambiente simultaneamente criativo e vulnerável. Nesse contexto, a educação hacker emerge como uma abordagem pedagógica capaz de formar mentes investigativas, críticas e éticas, fundamentadas na curiosidade e na autonomia intelectual. Longe da imagem estigmatizada do invasor digital, o hacker representa o sujeito que busca compreender sistemas, explorar possibilidades e construir soluções colaborativas. Como afirma Himanen (2001), a ética hacker valoriza o conhecimento como bem coletivo, a liberdade de criação e a responsabilidade ética diante da informação.

No campo da cibersegurança, essa perspectiva educacional ganha relevância ao propor uma

formação que ultrapassa a dimensão técnica, estimulando a reflexão sobre o uso ético das tecnologias. A lógica hacker se aproxima, nesse sentido, da pedagogia crítica de Freire (1996), ao defender a aprendizagem como prática de liberdade e de transformação social. Ensinar segurança digital, portanto, não é apenas treinar para proteger sistemas, mas promover uma cultura de consciência digital, de empatia tecnológica e de protagonismo ético.

Entre as metodologias que materializam essa visão, destacam-se as metodologias ativas, nas quais o estudante assume papel protagonista no processo de construção do conhecimento. Estratégias como a Problem-Based Learning (PBL) e a Challenge-Based Learning (CBL) se mostram eficazes para o ensino de cibersegurança, pois mobilizam a investigação, o trabalho em equipe e a tomada de decisão frente a desafios reais. Conforme Moran (2018), "a aprendizagem ativa é a ponte entre o saber e o fazer, entre o pensar e o transformar".

Nesse cenário, a gamificação surge como linguagem educativa capaz de integrar engajamento, motivação e experimentação. O uso de jogos no ensino de cibersegurança transcende o entretenimento e torna-se um espaço de simulação cognitiva, em que o erro é oportunidade de aprendizado e o desafio se converte em estímulo ao raciocínio crítico. Quando associada à educação hacker, a gamificação reforça valores como criatividade, ética e cooperação — fundamentos indispensáveis à formação de profissionais conscientes na era digital.

Entre as ferramentas que favorecem essa integração, o RPG Maker destaca-se por permitir a criação de narrativas interativas e ambientes simulados de aprendizagem. Seu potencial educacional reside na simplicidade de uso e na flexibilidade de design, possibilitando ao educador e ao estudante criar mundos virtuais que espelham dilemas éticos, ataques simulados e decisões críticas. Mais do que aprender sobre segurança, o aluno experimenta o processo de pensar como um analista — ou como um hacker ético — dentro de um contexto gamificado e narrativo.

Dessa forma, o presente artigo busca analisar a utilização do RPG Maker como ferramenta de gamificação e metodologia ativa no contexto da educação hacker, explorando sua aplicação teórica e pedagógica na formação crítica em cibersegurança. O objetivo é refletir sobre como o design de

jogos e narrativas interativas pode contribuir para o desenvolvimento de competências cognitivas, éticas e colaborativas, transformando o ato de aprender em um processo de investigação, criação e consciência digital.

REFERENCIAL TEÓRICO

O presente referencial teórico busca fundamentar a proposta da Educação Hacker articulada à gamificação com RPG Maker, com base em três eixos conceituais complementares: a ética hacker e a cultura do conhecimento livre, as metodologias ativas na formação em cibersegurança e o uso da gamificação como mediação pedagógica. Esses eixos sustentam a compreensão de que o aprendizado em segurança digital não deve limitar-se à dimensão técnica, mas envolver também uma dimensão ética, crítica e criativa. Assim, a literatura aqui revisada oferece o arcabouço necessário para compreender a intersecção entre autonomia intelectual, experimentação tecnológica e engajamento lúdico, elementos que estruturam a proposta educacional apresentada neste estudo.

Ética hacker e cultura do conhecimento livre

A educação hacker parte de uma ética que valoriza a curiosidade, o compartilhamento e a responsabilidade social no uso da tecnologia. Em oposição ao estereótipo do "invasor", a figura do hacker está vinculada à busca de compreensão profunda dos sistemas e à melhoria contínua de seu funcionamento (HIMANEN, 2001; LEVY, 2010). Essa postura aproxima-se de uma pedagogia crítica que vê o estudante como sujeito ativo da própria aprendizagem e como agente de transformação do contexto sociotécnico em que se insere (FREIRE, 1996). Assim, o termo hacker é menos um rótulo e mais um habitus investigativo, que combina competência técnica, autonomia intelectual e compromisso ético. A ética hacker, ao ser incorporada ao campo educacional, estimula a aprendizagem pela exploração, em que o erro é interpretado como oportunidade de descoberta e não como falha. Essa visão reforça

o caráter emancipador da tecnologia quando usada como meio de promover consciência crítica, colaboração e inovação social.

Metodologias ativas na formação em cibersegurança

As metodologias ativas deslocam o foco da transmissão de conhecimento para a investigação orientada a problemas e desafios, aproximando teoria e prática profissional (MORAN, 2018; DEMO, 2018). Na área da cibersegurança, estratégias como a Problem-Based Learning (PBL) e a Challenge-Based Learning (CBL) favorecem o raciocínio diagnóstico, a colaboração e a tomada de decisão sob incerteza — competências essenciais à análise de incidentes e à resposta a vulnerabilidades. A aprendizagem, nesse contexto, é concebida como um ciclo iterativo de exploração, tentativa, feedback e reflexão, no qual o erro informado é insumo didático e não fracasso, fortalecendo a autonomia e o pensamento crítico do aprendiz (GEE, 2003). Tais metodologias promovem não apenas a aquisição de competências técnicas, mas também a internalização de valores éticos e o desenvolvimento da resiliência diante de situações complexas e imprevistas.

Gamificação e RPG Maker como mediação pedagógica

A gamificação, entendida como a aplicação de elementos de jogos — objetivos, regras, feedback, narrativa, sistemas de pontuação e progressão — em contextos educacionais, potencializa engajamento, foco e persistência (DETERDING et al., 2011; KAPP, 2012; FADEL; TRILLING, 2019). No ensino de cibersegurança, os ambientes simulados e as narrativas interativas permitem encenar dilemas éticos, investigar ameaças e exercitar estratégias defensivas com baixo risco e alta relevância cognitiva.

O RPG Maker se destaca por sua baixa barreira de entrada e alta adaptabilidade pedagógica, permitindo que professores e estudantes criem narrativas interativas em que os desafios técnicos se

convertem em experiências de aprendizagem. No jogo, missões representam problemas de segurança a resolver; personagens simbolizam perfis de usuário e atacante; e sistemas de progressão refletem o avanço do aluno em competências como criptografia, análise forense e ética digital. O mapa do jogo funciona como metáfora espacial de uma infraestrutura de rede, enquanto puzzles e batalhas simbolizam a resolução de incidentes e a decisão ética frente a situações complexas.

Dessa forma, o RPG Maker atua como laboratório narrativo em que aprender sobre cibersegurança significa também exercitar julgamento moral, colaboração e documentação de descobertas.

Síntese teórica para o desenho didático

Da convergência entre ética hacker (valores), metodologias ativas (processos) e gamificação com RPG Maker (linguagem e ambiente) emerge um framework pedagógico hacker-crítico, que:

- Posiciona o estudante como investigador autônomo;
- Transforma conteúdos de cibersegurança em desafios narrativos interativos com feedback constante;
- Integra avaliação formativa contínua, com rubricas de desempenho, logs de análise e relatórios reflexivos

Esse referencial teórico sustenta a metodologia descrita na próxima seção, orientando o desenho da proposta educacional de aprendizagem ativa e gamificada para a formação crítica em cibersegurança.

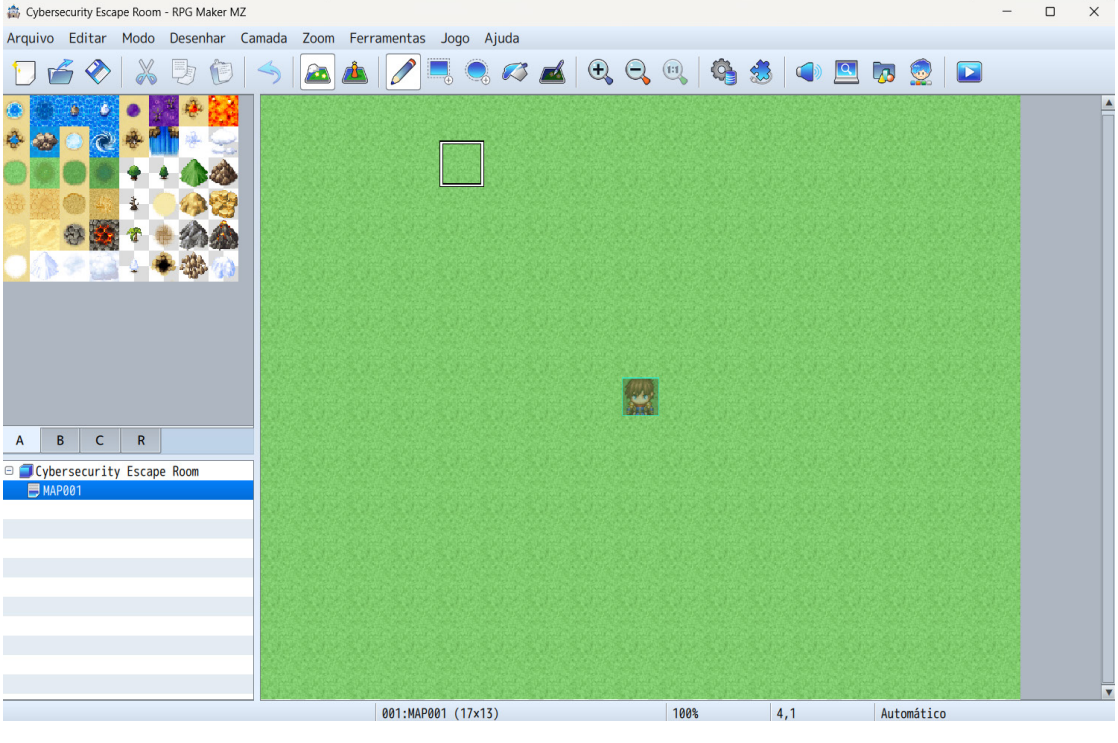
METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa qualitativa, teórico-aplicada e

exploratória, cujo objetivo é analisar e modelar o uso do RPG Maker como ferramenta de gamificação e metodologia ativa na Educação Hacker. A abordagem qualitativa permite compreender dimensões simbólicas, cognitivas e éticas do processo de aprendizagem, valorizando significados e interpretações emergentes nas interações entre aluno, narrativa e ambiente virtual (GIL, 2019; BARDIN, 2016).

De natureza aplicada, o estudo envolve o desenvolvimento, análise e validação reflexiva de um protótipo educacional baseado em narrativa interativa, no qual o estudante assume o papel de um agente ético de segurança digital. A criação do protótipo foi conduzida no RPG Maker MV, software que oferece ampla liberdade para elaborar mapas, eventos, diálogos, puzzles e sistemas de progressão.

Figura 1 - Ambiente de desenvolvimento do jogo no RPG Maker, com visualização de mapa, tileset e painel de eventos.



Fonte: elaboração própria (2025).

A metodologia foi estruturada em quatro etapas interdependentes, detalhadas a seguir.

Abordagem da pesquisa

A pesquisa adota a abordagem qualitativa, por permitir a exploração profunda de fenômenos educacionais complexos, especialmente aqueles relacionados a processos cognitivos, engajamento e ética no contexto da gamificação. O caráter teórico-aplicado decorre da criação de um artefato educacional (o jogo) articulado à análise conceitual da Educação Hacker, integrando fundamentos teóricos à experimentação prática.

Segundo Lakatos e Marconi (2020), pesquisas aplicadas visam transformar conhecimento teórico em soluções práticas. Assim, o RPG Maker funciona como objeto experimental, enquanto a revisão bibliográfica e a análise interpretativa fornecem o suporte epistemológico para compreender o papel do jogo na formação hacker.

A escolha dessa abordagem justifica-se porque jogos educacionais, por sua natureza simbólica e narrativa, exigem análise que ultrapassa a mensuração quantitativa e envolve compreensão crítica das experiências, decisões e interpretações dos jogadores.

Etapas de desenvolvimento do protótipo educativo

O processo de construção do protótipo no RPG Maker seguiu três fases principais:

Análise teórico-conceitual

Nesta etapa, foram identificados princípios centrais da ética hacker (HIMANEN, 2001), das metodologias ativas (MORAN, 2018; DEMO, 2018) e da gamificação (DETERDING et al., 2011; KAPP, 2012). Esses referenciais sustentaram as decisões de design pedagógico, determinando:

- valores éticos representados nos diálogos e escolhas do jogador;

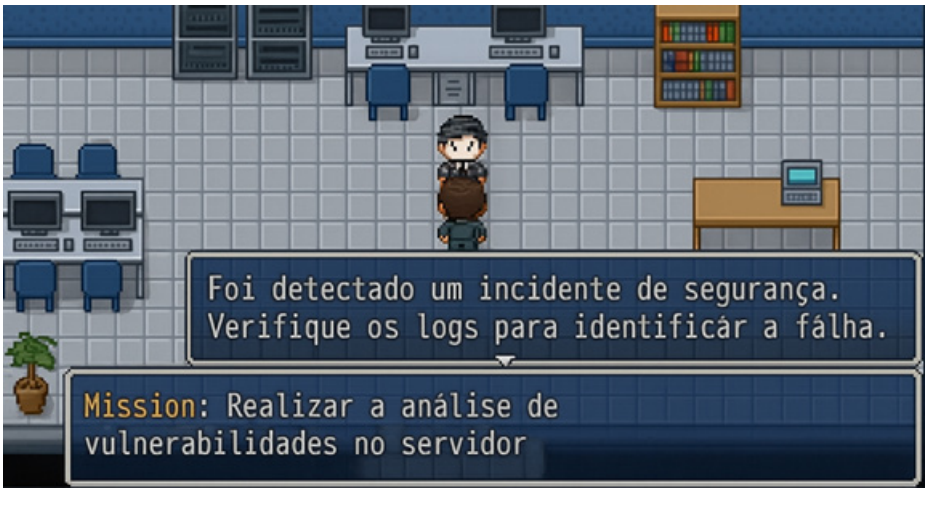
- desafios educativos estruturados como missões;
- lógicas de investigação associadas a puzzles e enigmas;
- retroalimentação formativa baseada em feedback narrativo.

Design pedagógico no RPG Maker

A segunda etapa consistiu na criação de um protótipo jogável, organizado em quatro missões formativas, cada uma representando uma competência essencial da Educação Hacker:

- Exploração e Reconhecimento – navegação inicial, coleta de pistas, identificação de vulnerabilidades.
- Análise Investigativa – leitura de logs simulados, quebra de códigos simples, análise de padrões.
- Resposta e Tomada de Decisão – escolha de ações éticas frente a dilemas e incidentes.
- Reflexão e Documentação – registro em diário digital, análise pós-incidente (post-mortem).

Figura 2 - Exemplo de Simulação a investigação de incidentes por meios de eventos e dialogos interativos



Fonte: elaboração própria (2025).

O RPG Maker foi escolhido devido à:

- facilidade de uso para educadores;
- possibilidade de criar simulações narrativas;
- linguagem visual que favorece compreensão;
- recursos de condicionais, variáveis e feedback imediatos.

Validação reflexiva e análise formativa

Após a construção do protótipo, realizou-se uma avaliação reflexiva sobre a eficácia didática das mecânicas, narrativa e progressão. Essa análise buscou identificar se o jogo:

- promove investigação e curiosidade;
- estimula raciocínio lógico e diagnóstico;
- reforça a ética hacker;
- incentiva colaboração e documentação.

A validação baseou-se em registros de eventos e decisões simuladas.

Figura 3 - Tela de feedback pedagógico que orienta decisões éticas e técnicas durante o jogo com multi-idioma

Fonte: Elaborado pela Autor

Instrumentos de análise

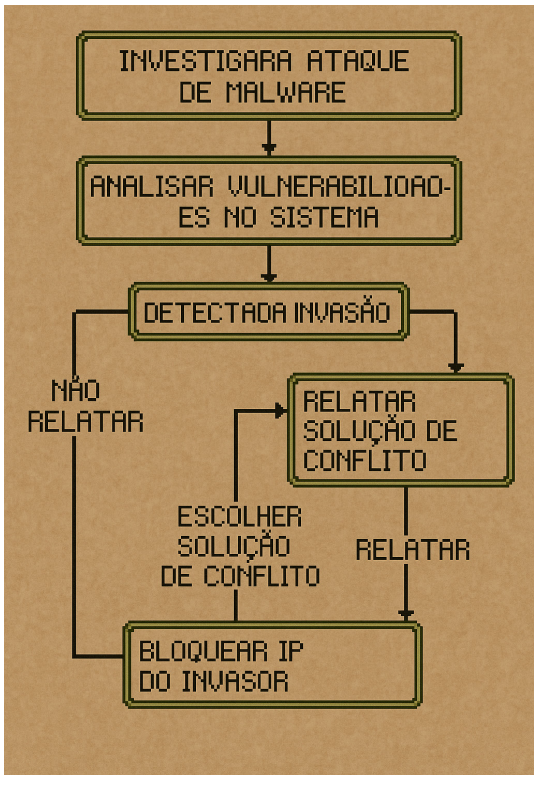
A interpretação dos dados seguiu o método de Análise de Conteúdo (BARDIN, 2016), permitindo organizar as evidências em três categorias avaliativas:

- Dimensão cognitiva – resolução de enigmas, análise de padrões, raciocínio técnico.
- Dimensão ética – tomada de decisão, consequências simuladas, alinhamento à ética hacker.
- Dimensão afetivo-motivacional – engajamento, persistência, curiosidade e autonomia.

Os instrumentos utilizados incluíram:

- logs de variáveis e eventos do RPG Maker;
- diário reflexivo do designer;
- mapas narrativos (storyboards) do jogo;
- roteiros de missão.

Figura 4 - Estrutura narrativa e lógica pedagógica das missões dentro do protótipo educacional.



Fonte: elaboração própria (2025).

Limitações metodológicas

Por ser uma pesquisa exploratória e aplicada, o estudo não realizou experimentação com turmas reais, o que limita a generalização dos resultados. Entretanto, a modelagem teórico-didática

do protótipo é suficiente para demonstrar:

- aplicabilidade do RPG Maker como ferramenta pedagógica;
- potencial formativo da Educação Hacker;
- coerência entre narrativa gamificada e desenvolvimento de competências.

Estudos futuros poderão aprofundar estas análises com aplicação em cursos técnicos e superiores, utilizando dados empíricos com estudantes de segurança da informação.

Assim, a metodologia empregada permitiu integrar princípios teóricos da ética hacker, estratégias de aprendizagem ativa e elementos de gamificação ao processo de desenvolvimento do protótipo educacional no RPG Maker. A articulação entre análise conceitual, design narrativo e validação reflexiva forneceu um arcabouço sólido para compreender como a experiência ludificada pode mediar o desenvolvimento de competências cognitivas, éticas e investigativas na formação em cibersegurança. Com base nesse percurso metodológico, apresentam-se a seguir os resultados obtidos a partir da construção do jogo e a discussão crítica sobre seu potencial pedagógico, evidenciando as contribuições da gamificação narrativa para a Educação Hacker.

RESULTADOS

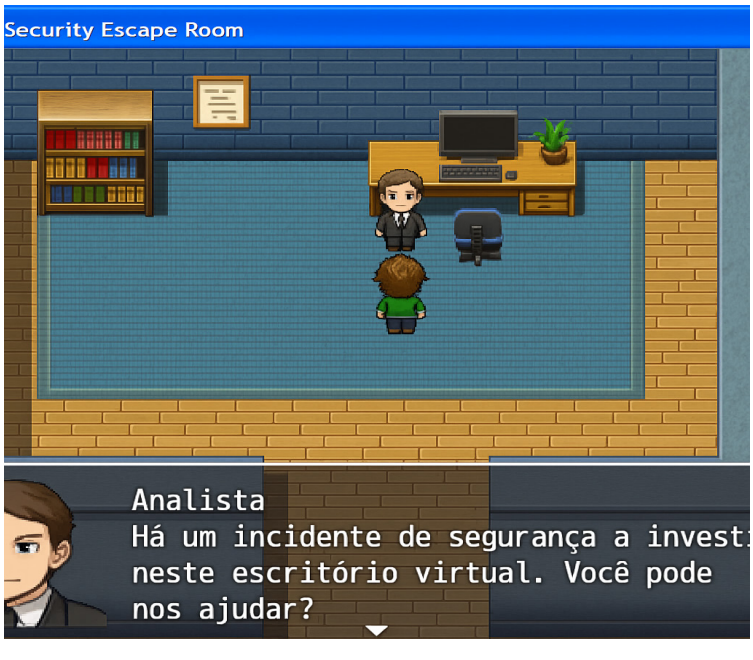
Os resultados deste estudo derivam da construção e análise do protótipo educacional CyberSecurity Escape Room, desenvolvido no RPG Maker MV como ambiente gamificado para a Educação Hacker. O protótipo foi concebido como uma experiência investigativa, narrativa e ética, em que o estudante assume o papel de um analista responsável por desvendar incidentes em um sistema digital fictício. A estrutura final apresentou quatro missões centrais, cada uma representando uma competência formativa essencial na área de cibersegurança: exploração, análise investigativa, tomada de decisão ética e reflexão pós-incidente.

A modelagem do CyberSecurity Escape Room demonstrou que o RPG Maker permite integrar narrativa, desafios lógicos e feedback pedagógico de maneira fluida, possibilitando a simulação de situações reais de segurança digital em um ambiente seguro, acessível e imersivo. A seguir, apresentam-se os principais resultados obtidos em relação às dimensões técnicas, pedagógicas e éticas do protótipo.

Estrutura narrativa do protótipo CyberSecurity Escape Room

A narrativa central do CyberSecurity Escape Room foi construída em torno do papel do aluno como investigador ético, responsável por rastrear comportamentos suspeitos e resolver enigmas distribuídos no ambiente virtual. O mapa principal representa um "sistema operacional fictício", dividido em setores como logs, rede, usuários e serviços críticos.

Figura 5 - Tela inicial do CyberSecurity Escape Room com o primeiro diálogo e ambiente de investigação



Fonte : Elaborado pelo Autor

Missões e desafios pedagógicos

O CyberSecurity Escape Room foi organizado em quatro missões pedagógicas:

Missão 1 – Reconhecimento e exploração

O jogador explora o "sistema", encontra pistas, analisa objetos interativos e conversa com NPCs (usuários e potenciais atacantes simulados).

Missão 2 – Análise investigativa

O aluno deve correlacionar logs, analisar pistas, decifrar códigos simples e resolver puzzles estruturados como evidências digitais.

Figura 6 - Enigma investigativo do CyberSecurity Escape Room vinculado à Missão 2

Fonte: Elaboração do Autor

Missão 3 – Tomada de decisão ética

Escolhas morais influenciam o desfecho da narrativa. As decisões são registradas por variáveis internas do RPG Maker, compondo um sistema de pontuação ética.

Missão 4 – Reflexão e documentação

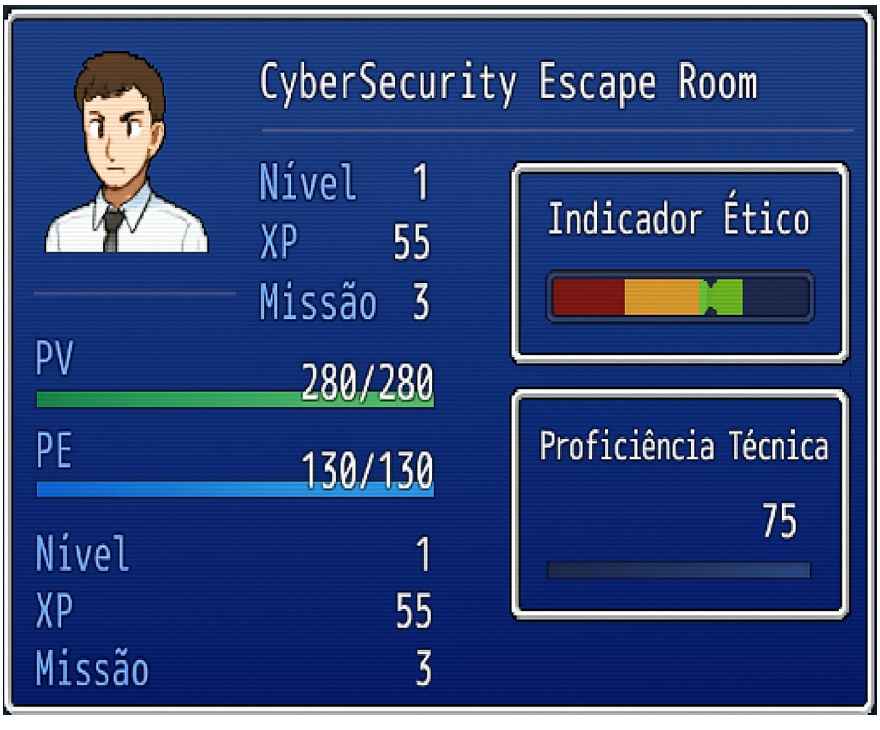
O jogador registra suas conclusões em um diário simulado, reforçando práticas de post-mortem e documentação.

Elementos de gamificação implementados no protótipo

No CyberSecurity Escape Room, foram implementados elementos clássicos de gamificação:

- feedback imediato;
- narrativa ramificada;
- sistema de progresso (pontos éticos, indicadores de investigação);
- desafios graduais;
- objetivos explícitos por missão.

Figura 7 - Sistema de progressão do CyberSecurity Escape Room mostrando indicadores éticos e técnicos



Fonte: Elaborado pelo Autor

Dimensões cognitivas observadas

O protótipo estimulou especialmente:

- Raciocínio investigativo — análise de pistas e padrões.
- Pensamento ético — escolha de ações com consequências narrativas.
- Autonomia exploratória — liberdade para navegar e testar hipóteses.

Além dessas dimensões, observou-se efeito positivo no pensamento sistêmico, uma vez que o aluno aprende a reconhecer relações entre eventos, ambientes e indícios, reproduzindo a lógica de investigação usada em contexto profissional de cibersegurança.

Potencial pedagógico identificado

A análise indica que o CyberSecurity Escape Room:

- facilita compreensão de fundamentos de cibersegurança;
- coloca o aluno como protagonista da investigação;
- integra valores da ética hacker ao aprendizado;
- promove engajamento e pensamento crítico;
- serve como ambiente seguro para treinar decisões em cenários complexos.

O protótipo mostrou-se especialmente eficaz em aproximar os estudantes da mentalidade investigativa, que é um dos pilares da formação hacker ética.

Os resultados obtidos com o desenvolvimento do CyberSecurity Escape Room evidenciam o potencial do RPG Maker como ferramenta de gamificação e mediação cognitiva na formação em cibersegurança. A integração entre narrativa, desafios e tomada de decisão oferece uma experiência que vai além da aprendizagem técnica, promovendo reflexão ética, curiosidade investigativa e protagonismo do estudante. Com base nesses achados, a próxima seção apresenta uma discussão crítica, relacionando os resultados com a literatura sobre ética hacker, metodologias ativas e gamificação, a fim de compreender como essas dimensões se articulam para a formação crítica em segurança digital.

DISCUSSÃO

Os resultados obtidos com o desenvolvimento do protótipo CyberSecurity Escape Room evidenciam que a gamificação narrativa pode assumir papel central na Educação Hacker ao integrar competências técnicas, éticas e investigativas em um único ambiente formativo. Tal integração dialoga

diretamente com a perspectiva de Himanen (2001), para quem a ética hacker é construída sobre a curiosidade, a autonomia e o compromisso ético com o conhecimento. No protótipo, esses elementos se manifestam por meio da exploração livre, da resolução de desafios investigativos e das decisões que influenciam o curso da narrativa. O aluno não apenas descobre falhas ou resolve enigmas: ele compreende que cada ação tem implicações éticas, reforçando a responsabilidade que caracteriza o agir hacker.

Na perspectiva das metodologias ativas, o CyberSecurity Escape Room opera como ambiente de investigação orientada a problemas, alinhado ao que Moran (2018) defende como aprendizagem significativa baseada na autonomia do estudante. Ao enfrentar desafios progressivos, o aluno mobiliza raciocínio lógico, correlação de evidências e tomada de decisão sob incerteza — habilidades fundamentais na análise de incidentes e na resposta a vulnerabilidades. A narrativa gamificada, ao estruturar esses desafios em forma de missões, transforma o conteúdo técnico em experiência vivida, permitindo que o estudante "aprenda fazendo", em consonância com a pedagogia de Freire (1996), que compreende o conhecimento como prática emancipatória.

A análise das escolhas éticas na Missão 3 mostra que a gamificação não se limita à dimensão técnica. Ela também pode ser um meio para representar dilemas reais da cibersegurança, como a responsabilidade sobre uma vulnerabilidade descoberta ou o impacto de uma decisão precipitada. Esses elementos aproximam o jogo de discussões mais amplas sobre ética algorítmica e responsabilidade digital, conforme defendido por Paes (2025), ao afirmar que a educação tecnológica deve formar sujeitos capazes de refletir criticamente sobre o poder e os riscos das tecnologias contemporâneas. No CyberSecurity Escape Room, essa reflexão emerge não como tema abstrato, mas como consequência de escolhas incorporadas à narrativa.

Já a análise das dimensões cognitivas observadas no protótipo confirma o potencial educativo dos jogos quando construídos com intencionalidade pedagógica. Gee (2003) destaca que jogos bem estruturados promovem ciclos contínuos de ação–reflexão–avaliação, estimulando pensamento crítico e resolução de problemas complexos. Essa dinâmica é visível no protótipo desenvolvido: o aluno

experimenta hipóteses, testa ações, recebe feedback imediato e ajusta sua estratégia — processos essenciais para o desenvolvimento da competência investigativa em cibersegurança.

No que diz respeito à gamificação, os resultados demonstram consonância com o modelo de Deterding et al. (2011), que compreende a gamificação como aplicação de elementos de jogos com propósito formativo, e não meramente lúdico. No CyberSecurity Escape Room, sistemas de pontuação, narrativa ramificada e feedback ético foram integrados ao design instrucional com objetivo de promover engajamento cognitivo e reflexão crítica. O jogo não recompensa o aluno por acumular pontos, mas por tomar decisões coerentes, investigar pistas e agir eticamente — o que fortalece a compreensão de que, na Educação Hacker, o processo importa mais do que o resultado.

O potencial pedagógico do protótipo também confirma o argumento de Fadel e Trilling (2019), segundo o qual ambientes digitais interativos podem favorecer a aprendizagem de competências do século XXI, como pensamento crítico, criatividade e resolução colaborativa de problemas. Embora o protótipo não tenha sido aplicado a grupos reais, sua análise interna já demonstra que o design de jogo pode atuar como mediador cognitivo altamente eficaz ao simular cenários complexos de cibersegurança sem expor estudantes a riscos reais.

Por fim, ao incorporar a lógica de escape room e elementos investigativos, o protótipo dialoga com a noção de que o jogo pode ser entendido como "espaço seguro de experimentação" (KAPP, 2012). Nele, o erro deixa de ser penalização e torna-se oportunidade de aprendizagem — princípio que se alinha profundamente à cultura hacker, para a qual explorar, testar, falhar e aprender são etapas inseparáveis do desenvolvimento do conhecimento.

Dessa forma, a discussão dos resultados revela que o CyberSecurity Escape Room não apenas simula situações de cibersegurança, mas forma modos de pensar, ajudando o estudante a internalizar práticas éticas, investigativas e reflexivas que caracterizam o espírito hacker. O jogo transforma o estudante de espectador passivo em agente crítico, capaz de analisar, decidir e aprender em ciclos contínuos de ação e reflexão.

CONCLUSÃO

Os resultados obtidos ao longo deste estudo mostram que a integração entre Educação Hacker, metodologias ativas e gamificação narrativa, materializada no protótipo CyberSecurity Escape Room, representa uma abordagem pedagógica potente para o ensino de cibersegurança. A construção do jogo demonstrou que o RPG Maker é uma ferramenta capaz de articular exploração investigativa, tomada de decisão ética e resolução de problemas técnicos em um ambiente seguro e imersivo. Nesse sentido, evidencia-se que o design narrativo de um escape room digital não apenas engaja os estudantes, mas também promove o desenvolvimento de competências críticas para a área, como pensamento analítico, raciocínio lógico, interpretação de evidências e postura ética diante de dilemas reais.

A análise do protótipo reforça a compreensão de que a Educação Hacker vai além do domínio técnico; ela envolve uma formação integral que inclui autonomia, responsabilidade e reflexão sobre o impacto das ações em ambientes digitais. A gamificação, quando aplicada com intencionalidade pedagógica, pode potencializar esses processos, criando desafios significativos e contextos narrativos que estimulam ações conscientes. As missões estruturadas no CyberSecurity Escape Room demonstraram que ambientes lúdicos podem favorecer o protagonismo estudantil, permitir o teste seguro de hipóteses e aproximar situações reais de investigação forense do cotidiano formativo.

Além disso, observa-se que essa abordagem se alinha aos princípios das metodologias ativas, especialmente ao learning by doing e à aprendizagem baseada em desafios. O estudante deixa de ser receptor de conteúdos e torna-se agente de suas próprias descobertas, navegando por problemas complexos que exigem análise crítica e tomada de decisão. Esse deslocamento contribui para a formação de profissionais mais preparados para atuar em um campo dinâmico e em constante mutação, como é a cibersegurança.

Por fim, conclui-se que a combinação entre ética hacker, narrativa interativa e gamificação representa um caminho promissor para inovar no ensino de cibersegurança. O protótipo desenvolvido

não se limita a ser uma ferramenta de entretenimento, mas constitui um espaço pedagógico que estimula autonomia, criticidade e responsabilidade digital. Recomenda-se que pesquisas futuras ampliem essa proposta para aplicações colaborativas, experiências multiplataforma e avaliações empíricas com grupos de estudantes, de modo a validar e expandir o potencial formativo identificado neste estudo. Assim, o CyberSecurity Escape Room se apresenta como uma contribuição relevante e inovadora para a formação de sujeitos capazes de compreender, investigar e proteger sistemas digitais na sociedade contemporânea.

REFERÊNCIAS

OLIVEIRA, Sérgio Luiz. Perícia digital e educação tecnológica: desafios do ensino investigativo. Brasília: Editora IFB, 2022.

BARDIN, Laurence. Análise de conteúdo. São Paulo: Edições 70, 2016.

DETERDING, Sebastian et al. From Game Design Elements to Gamefulness: Defining "Gamification". In: Proceedings of the 15th International Academic MindTrek Conference, 2011. p. 9–15.

DEMO, Pedro. Metodologia para quem quer aprender. 2. ed. São Paulo: Atlas, 2018.

FADEL, Charles; TRILLING, Bernie. Educação para o século XXI: competências para o futuro. Porto Alegre: Penso, 2019.

FREIRE, Paulo. Pedagogia da autonomia: saberes necessários à prática educativa. São Paulo: Paz e Terra, 1996.

GEE, James Paul. What Video Games Have to Teach Us About Learning and Literacy. New York: Palgrave Macmillan, 2003.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 7. ed. São Paulo: Atlas, 2019.

HIMANEN, Pekka. A ética do hacker e o espírito da era da informação. Rio de Janeiro: Campus,

2001.

KAPP, Karl M. The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. San Francisco: Pfeiffer, 2012.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 8. ed. São Paulo: Atlas, 2020.

LEVY, Steven. Hackers: Heroes of the Computer Revolution. 25th Anniversary Edition. Sebastopol: O'Reilly Media, 2010.

MORAN, José. Metodologias ativas para uma aprendizagem inovadora. São Paulo: Mackenzie, 2018.

PAES, Tadeu Marcos Borges. Singularidade Tecnológica Educacional: O Salto Temporal – Uma Revolução Inevitável. Belém: AlphaNexus Academy, 2025.