

# Cyber Resistance: Protótipo de jogo educacional para ensino de segurança cibernética

**Maria Vitória Polido de Souza, Juliano Rubio Sangaleti, Rodrigo Campiolo,  
Marcos Silvano Almeida, Luiz Arthur Feitosa dos Santos**

Universidade Tecnológica Federal do Paraná (UTFPR)  
Campo Mourão - PR - Brasil

{mariavitoriasouza, julianosangaleti}@alunos.utfpr.edu.br  
{rcampiolo, marcossilvano, luizsantos}@utfpr.edu.br

**Abstract.** This article presents ongoing work on the development and evaluation of an educational game aimed at promoting cybersecurity learning. The scenarios and characters are being developed using the Godot engine, following an incremental and modular process to enable the integration of various gamified activities. As partial results, the initial scenario and characters have been created, along with gamified quiz and logic challenge activities. The game has shown promising outcomes in a preliminary evaluation conducted with Computer Science students.

**Resumo.** Este artigo aborda o desenvolvimento e avaliação de um jogo educacional voltado para o aprendizado de cibersegurança. Os cenários e personagens estão sendo desenvolvidos em Godot, seguindo um processo incremental e modular, de forma a propiciar o acoplamento de diferentes atividades gamificadas. Como resultados parciais, foram desenvolvidos o cenário inicial e personagens, atividades de quizzes e desafios lógicos. O jogo mostrou-se promissor em uma avaliação preliminar com estudantes.

## 1. Introdução

A cibersegurança tem ganhado cada vez mais notoriedade em uma sociedade cada vez mais conectada. A dependência da Internet traz riscos em diferentes níveis (pessoais, organizacionais e nacionais), evidenciando a urgência de proteção contra ciberameaças.

Nesse sentido, a educação em cibersegurança é fundamental para formar esses profissionais. Entretanto, a natureza multidisciplinar e complexa da área representa um grande desafio, desestimulando estudantes a seguir essa área. Uma abordagem moderna e promissora para engajar os estudantes é o uso de jogos eletrônicos na educação [Dicheva et al., 2015], que podem ser usados para manter a motivação dos estudantes.

Desta forma, no que diz respeito à cibersegurança, há vários tipos de jogos já desenvolvidos direcionados para aprendizados básicos e/ou específicos [Weitl-Harms et al., 2023]. Contudo, não é seguido um currículo que vise a formação geral de estudantes em cibersegurança. Esses jogos apresentam-se mais como ferramentas para aperfeiçoamento em diferentes tópicos isolados da área.

Considerando a importância da cibersegurança e a necessidade de formar profissionais qualificados na área, propõe-se o desenvolvimento de um jogo eletrônico que aborda os aspectos educacionais e as etapas de formação de profissionais em cibersegurança.

## 2. Revisão da Literatura

Esta revisão apresenta conceitos-chave e trabalhos correlatos que norteiam a proposta deste projeto, os quais são: a gamificação na educação, gamificação no ensino de cibersegurança e jogos eletrônicos associados à cibersegurança.

A gamificação, conforme definida por Deterding et al. (2011), consiste no uso de elementos de jogos em outras aplicações ou contextos. Por sua vez, esses elementos podem ser aplicados na educação, visto que atacam dois dos principais desafios no ensino: motivação e engajamento [Lee, J.; Hammer, J., 2011]. Além disso, promovem o desenvolvimento de qualidades como persistência, criatividade e resiliência.

Outro conceito-chave relacionado com a gamificação é o de jogos sérios (*serious games*), que referem-se a jogos completos, projetados com o propósito principal que não o puro entretenimento, enquanto as aplicações gamificadas usam os elementos dos jogos, e não necessariamente o jogo completo [Deterding et al., 2011]. Na categoria de jogos sérios, destacam-se os jogos educacionais.

Em geral, verifica-se na literatura que os jogos educacionais e a gamificação aplicados ao ensino são fatores que somam para o aumento do engajamento e facilidade de aprendizado dos alunos. Sabe-se que a cibersegurança é uma área complexa que envolve o conhecimento avançado e aprofundado em diferentes áreas da Computação; por isso, o uso da gamificação e jogos para o ensino de cibersegurança já vem sendo investigado e usado na prática por organizações e academia.

Weitl-Harms et al. (2023) apresentam um mapeamento sistemático de aplicações gamificadas aplicadas à educação em cibersegurança. Analisaram 74 trabalhos publicados entre 2007 e 2022, os quais incluíam avaliações no ensino de graduação. Há também diferentes jogos eletrônicos com temática em cibersegurança: Hacknet [Hacknet, 2024], Bitburner [Xie, 2016], OverTheWire [Overthewire, 2024], CyberCIEGE [Irvine, 2005; Cybersiege, 2024]. Alguns apresentam como ponto principal a história (p. ex. Hacknet), mecânicas realistas (p. ex. OverTheWire), ambientes 3D (p. ex. CyberCIEGE), programação de *scripts* (p. ex. Bitburner).

O CyberCIEGE se destaca por seu uso em treinamentos de cibersegurança em organizações e por ser o discutido em publicações da área. No entanto, em geral, nenhum dos jogos apresenta uma proposta de ensino linear para formar profissionais em cibersegurança.

## 3. Materiais e Métodos

O jogo *Cyber Resistance* está sendo desenvolvido na Godot Engine [Godot, 2025], uma plataforma *open source* que recebe atualizações com frequência (atualmente, é utilizada a versão 4.4 da engine). Optou-se majoritariamente por GDScript, a linguagem nativa da Godot; no entanto, também há a possibilidade de utilizar C#, o que proporciona flexibilidade para funcionalidades futuras.

Quanto à organização, foi utilizado o GitHub [Github, 2025] para versionamento de código e controle de repositórios. Paralelamente, o Notion [Notion, 2025] tem sido essencial para o registro de ideias, planejamento de tarefas, cronogramas e documentação geral do projeto.

O jogo faz uso de uma estética retrô em *pixel art*, que está sendo desenvolvida no LibreSprite [Libresprite, 2025]. O jogo é 2D, com perspectiva *top-down*. Essas escolhas foram inspiradas em jogos clássicos, como Stardew Valley [Barone, 2025], que equilibram tanto a estética quanto a jogabilidade.

O método de desenvolvimento é incremental e modular. No entanto, visando um aprendizado linear em cibersegurança, ou seja, que progride de conceitos simples aos complexos, a primeira etapa concentrou-se na criação de cenários, personagens e mecânicas, além de planejar a integração incremental das atividades gamificadas.

Logo, os passos realizados até o momento foram:

1. Revisão da literatura para identificação e resumo dos principais trabalhos na área de gamificação aplicados ao ensino no contexto de cibersegurança;
2. Identificação e comparação dos jogos educacionais existentes que tratam de cibersegurança;
3. Estudo das tecnologias para o desenvolvimento de jogos, técnicas para projeto de cenários e personagens;
4. Elaboração de elementos gráficos de cenários e personagens, em conjunto com a implementação das mecânicas do jogo: interação dos personagens, modificação de ambientes, execução de atividade gamificada, entre outros;
5. Avaliação do protótipo do jogo com alunos de cursos de Computação: avaliação do projeto gráfico e interação dos usuários com o jogo.

O protótipo ainda está em uma versão preliminar, mas já possibilita a adição de atividades gamificadas simples, como problemas lógicos e quizzes.

## 4. Resultados Preliminares

No estado atual da pesquisa, foram realizadas a construção do cenário inicial, constituído de Cafeteria e Universidade, a implementação do modelo-base dos NPCs (*Non-Player Character*) e a avaliação preliminar do jogo e de atividade gamificada com alunos do primeiro ano do curso de Ciência da Computação.

### 4.1. Enredo, cenários e personagens

O enredo do jogo envolve um aluno (jogador) que acaba de ingressar na universidade e acaba sendo recrutado para auxiliar a Resistência no combate a uma organização que controla o mundo por meio de tecnologias de informação. Durante sua jornada, o jogador deverá desenvolver suas habilidades em lógica, programação, redes de computadores, sistemas operacionais e cibersegurança para realizar as missões.

A Figura 1 apresenta o mapa do jogo e o jogador no cenário da cafeteria diante do computador que provê acesso a máquinas reais e outras atividades gamificadas.



**Figura 1. Mapa da cidade e jogador (personagem)**

Destaca-se como um aspecto importante do jogo, as atividades a serem realizadas em cenários reais simulados, conectando-se a máquinas virtuais e/ou contêineres via a interface do computador. Todo computador no jogo oferece acesso a uma interface que permite ao jogador realizar atividades de segurança ofensiva e defensiva.

Na configuração de diálogos, missões e quizzes foram utilizados arquivos JSON. No caso dos diálogos, os arquivos armazenam a identificação do NPC com seus diálogos possíveis. Esses diálogos são classificados como aleatórios ou específicos. Para os específicos, definem-se o nome da missão, o estado para ativação do diálogo, entre outros atributos.

Uma das dificuldades encontradas foi a transição entre cenas, especialmente quando o jogador acessa o computador (representado por uma nova cena). Como solução, foi criado um *Autoload* chamado *Global.gd*, responsável por gerenciar a cena atual e a anterior, garantindo que a posição do jogador seja mantida corretamente.

#### 4.3. Avaliação do Jogo e da Atividade Gamificada

A avaliação do jogo e da atividade gamificada foi realizada com 41 alunos do primeiro ano de Ciência da Computação, durante uma aula de aproximadamente 1 hora e 30 minutos, no laboratório de Informática.

O processo de avaliação consistiu na apresentação do jogo, seguida da instalação e execução individual por cada participante. No jogo, os objetivos foram: conhecer o cenário e controles, conversar com os NPCs e realizar missões. As principais missões foram resolver o anagrama no computador da cafeteria e responder o quiz sobre cibersegurança.

Ao final do processo, os participantes responderam um questionário de avaliação sobre o jogo (<https://forms.gle/KFmAtuwErxFq7fK6>) contendo 5 questões objetivas, 4 dissertativas e realizaram o *upload* das respostas do quiz. Optou-se por um conjunto reduzido de questões, devido ao perfil dos participantes e pelo uso de versão preliminar

do jogo. As perguntas foram baseadas nos processos de avaliação descritos por [Rocha et al., 2015] e [Catalano et al., 2014].

As questões objetivas mostram que elementos como enredo, mecânica, personagens e os desafios despertaram interesse dos alunos pelo jogo, pois 63,4% demonstraram muito interesse pelo jogo. Em relação à área de cibersegurança, 46,3% apresentaram muito interesse, 48,8% pouco interesse e apenas 4,9% sem interesse. Além disso, a percepção com relação ao estudo foi positiva, mesmo no caso de erros de resposta do aluno. O retorno de *feedback* auxiliou mais de 82,9% dos participantes na compreensão das questões.

Nas questões dissertativas, verificou-se que a arte e a jogabilidade agradaram a maioria dos participantes. Um resultado não esperado foi o elogio quanto ao desafio do anagrama que, inicialmente pensou-se que causaria desengajamento, e ocorreu o contrário. Foram dadas sugestões de melhorias como: mini-mapa, otimização da taxa de quadros e dicas para auxiliar nos desafios, o que pode melhorar a jogabilidade e engajamento para alguns dos participantes.

O quiz continha 10 questões aleatórias organizadas em 4 tópicos: segurança de senhas, autenticação e autorização, ataques cibernéticos, ferramentas e práticas de segurança. As questões eram básicas devido ao perfil dos participantes. Os resultados foram: 10 participantes acertaram todas as questões e a média de acerto por participante foi de 50,2%, destacando que o tópico com maior número de erros foi segurança de senhas. Para garantir a motivação e dedicação dos participantes na avaliação, esses foram recompensados com pontos de participação na disciplina e premiação (guloseimas) para as maiores pontuações no quiz.

## 5. Considerações Finais

Como parte da primeira etapa do projeto, foi desenvolvido e avaliado preliminarmente um protótipo inicial e jogável do Cyber Resistance. Os resultados da avaliação são promissores, visto que os estudantes gostaram do enredo, arte e atividades gamificadas. Além disso, os *feedbacks* nortearão decisões de projeto e a implementação de novas atividades no jogo.

Como trabalhos futuros desta primeira etapa de pesquisa, planeja-se adicionar uma atividade gamificada mais desafiadora e que exigirá conhecimentos de sistemas operacionais e cibersegurança. A ideia é que o jogo com essa nova atividade, seja avaliada pelos alunos da disciplina de cibersegurança.

## 6. Agradecimentos

Agradecemos à Fundação Araucária pelo apoio financeiro concedido por meio de bolsa de Iniciação Tecnológica a Juliano Rubio Sangaleti.

## Referências

- BARONE, Eric. Stardew Valley [jogo eletrônico]. ConcernedApe. Microsoft Windows: Chucklefish, 2016. Disponível em: <https://www.stardewvalley.net>. Acesso em: 20/05/2025.
- CATALANO, Chiara Eva Catalano; LUCCINI, Angelo Marco Luccini; MORTARA, Michela Mortara et al. Best Practices for an Effective Design and Evaluation of Serious Games. International Journal of Serious Games, v. 1, n. 1, January, 2014.
- CYBERSIEGE. CyberSiege, 2024. Disponível em: <https://nps.edu/web/c3o/cyberciege>. Acesso em 03/04/2024.
- DETERDING, S.; KHALED, R.; NACKE, L. E.; DIXON, D. Gamification: Toward a definition. In: CHI 2011 Gamification Workshop Proceedings. 2011.
- DICHEVA, D.; DICHEV, C.; AGRE, G.; ANGELOVA, G. Gamification in education: A systematic mapping study. Journal of educational technology & society, v. 18, n. 3, p. 75–88, 2015. JSTOR.
- GITHUB, Inc. GitHub: Where the world builds software. Disponível em: <https://github.com/>. Acesso em: 20/05/2025.
- GODOT. Godot Engine – Free and open source 2D and 3D game engine. Disponível em: <https://godotengine.org/>. Acesso em: 20/05/2025.
- HACKNET. Hacknet., 2024. Disponível em: <https://hacknet-os.com/>. Acesso em 03/04/2024.
- IRVINE, C. E.; THOMPSON, M. F.; ALLEN, K. CyberCIEGE: gaming for information assurance. IEEE Security & Privacy, v. 3, n. 3, p. 61–64, 2005. IEEE.
- LEE, J.; HAMMER, J. Gamification in Education: What, How, Why Bother? Academic Exchange Quarterly, 2011.
- LIBRESPRITE. LibreSprite: Animated sprite editor & pixel art tool. Disponível em: <https://libresprite.github.io/>. Acesso em: 20/05/2025.
- NOTION, Inc. Notion – One workspace. Disponível em: <https://www.notion.so/>. Acesso em: 20/05/2025.
- OVERTHEWIRE. OverTheWire: Wargames., 2024. Disponível em: <https://overthewire.org/>. Acesso em 03/04/2024.
- ROCHA, R. V. da; BITTENCOURT, I. I.; ISOTANI, S. Avaliação de jogos sérios: questionário para autoavaliação e avaliação da reação do aprendiz. Anais do SBGames, 2015.
- WEITL-HARMS, S.; SPANIER, A.; HASTINGS, J.; ROKUSEK, M. A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education. Journal of Cybersecurity Education, Research and Practice, v. 2023, n. 1, 2023.
- XIE, D. Bitburner. , 2016. Disponível em: <https://danielyxie.github.io/bitburner/>. Acesso em 03/04/2024.

## Apêndice A

A Figura 2 apresenta a interação entre o jogador e o professor. Observa-se o menu de missões no canto superior esquerdo e diálogos na parte inferior da tela. Um aspecto importante são as recompensas: classificação no jogo, nota extra em disciplina, acesso a fases avançadas/secretas, entre outros.



**Figura 2. Interação do jogador com personagens do jogo.**

A Figura 3 apresenta a tela de interação do jogador com o computador.



**Figura 3. Interface para interação com ambientes reais virtualizados/conteinerizados.**