Cyber Defender: desenvolvimento e avaliação de um jogo educativo para ensino de segurança cibernética

Cyber Defender: Development and Evaluation of an Educational Game for Teaching Cybersecurity

Eduardo Emilio dos Santos[1], Maurilio Martins Campano Junior[1,2], Felippe Fernandes da Silva[1], Linnyer Beatrys Ruiz Aylon[1]

[1]Universidade Estadual de Maringá (UEM)
Departamento de Informática (DIN)
Programa de Pós-Graduação em Ciência da Computação (PCC)
Manna_team
Maringá - PR - Brazil

[2]Centro Universitário UniCesumar
Engenharia de Software
Maringá - PR - Brazil

eduardoemilio122@gmail.com, maurilio.campanojr@gmail.com,
felippefernandes10@gmail.com, lbruiz@uem.br

Abstract. *The advancement of technology and the increasing reliance on digital systems highlight the importance of information security education, especially among students and future computing professionals. In this context, this study presents the design, development, and evaluation of the educational game Cyber Defender, conceived with the aim of supporting the teaching of fundamental digital security concepts in a playful and interactive manner. To assess the game, four well-established methodologies from the literature on educational game evaluation were applied: MEEGA+, IAQJEd, Pro-Avalia JS, and PAJED. The analyses covered aspects such as usability, gameplay, user experience, educational impact, narrative, and accessibility. The results demonstrate that the game features a well-structured narrative, satisfactory gameplay, and strong alignment with the proposed educational objectives, in addition to presenting a high learning potential according to the criteria of the applied methodologies.*
Keywords. *educational game, cybersecurity, educational game evaluation*

Resumo. *O avanço da tecnologia e a crescente dependência de sistemas digitais evidenciam a importância da educação em segurança da informação, especialmente entre estudantes e futuros profissionais da computação. Considerando esse cenário, este trabalho apresenta o projeto, desenvolvimento e avaliação do jogo educativo Cyber Defender, concebido com o objetivo de apoiar o ensino de conceitos fundamentais de segurança digital de forma lúdica e interativa. Para a avaliação do jogo, foram aplicadas quatro metodologias consolidadas na literatura para análise de jogos educacionais: MEEGA+, IAQJEd, Pro-Avalia JS e PAJED. As análises contemplaram aspectos como usabilidade, jogabilidade, experiência do usuário, impacto*

educacional, narrativa e acessibilidade. Os resultados obtidos demonstram que o jogo possui uma narrativa bem estruturada, jogabilidade satisfatória e bom alinhamento com os objetivos educacionais propostos, além de apresentar elevado potencial de aprendizagem segundo os critérios das metodologias aplicadas.
Palavras-chave. *jogo educativo, cibersegurança, avaliação de jogo educativo*

1. Introdução

A computação é uma área do conhecimento ampla e multifacetada, que abrange disciplinas como algoritmos e estruturas de dados, engenharia de software e desenvolvimento de sistemas. Com o avanço contínuo da tecnologia, sua presença tornou-se indispensável em diversos setores da sociedade, como saúde, finanças, educação e segurança [Paschoal et al. 2020].

O aumento expressivo da adoção de tecnologias digitais tem impactado diretamente o cenário da cibersegurança, tornando-o cada vez mais desafiador. Em 2024, por exemplo, as ferramentas de proteção da Kaspersky bloquearam mais de 300 milhões de tentativas de infecção por *malwares*, além de identificarem e impedirem o acesso a inúmeras URLs maliciosas, objetos perigosos em páginas da *web* e ataques de *ransomware* [Kaspersky 2024]. Esses números revelam a crescente sofisticação e frequência das ameaças virtuais, evidenciando a necessidade de iniciativas educativas voltadas à segurança da informação.

Diversos estudos reforçam a vulnerabilidade dos usuários diante dos riscos digitais, apontando práticas inadequadas, como a utilização de senhas frágeis [Aljohani et al. 2020], a alta suscetibilidade a ataques de *phishing* [Syafitri et al. 2022] e a falta de percepção sobre o monitoramento de suas atividades online por meio de cookies [Lin et al. 2023].

Nesse contexto, os jogos surgem como ferramentas promissoras no processo educativo. Definidos como sistemas artificiais delimitados por regras, nos quais os jogadores se engajam voluntariamente e que apresentam indicadores claros de vitória e derrota, os jogos se caracterizam pela interatividade, imersão e *feedback* automático [Gris e Souza 2016]. Jogos educativos, em particular, integram essas características com objetivos pedagógicos, buscando promover a aprendizagem de comportamentos e conhecimentos específicos. Estudos demonstram a eficácia dos jogos educativos na facilitação do processo de aprendizagem e na capacitação de grandes públicos [Panosso et al. 2015]; [Tsutsumi et al. 2020].

Diante desse cenário, este trabalho apresenta o projeto, desenvolvimento e avaliação do jogo educativo *Cyber Defender*, voltado para o ensino de conceitos fundamentais de segurança digital. A avaliação do jogo foi realizada por meio de quatro metodologias consolidadas na literatura, cujos resultados indicam uma narrativa consistente, jogabilidade satisfatória e uma abordagem eficiente dos conteúdos educativos propostos.

O restante deste trabalho apresenta os Trabalhos Relacionados na Seção 2, o projeto e o desenvolvimento do jogo Cyber Defender são descritos nas Seções 3 e 4. Já os resultados e análise das avaliações são apresentados na Seção 5 e as Conclusões e Trabalhos Futuros podem ser visualizados na Seção 6.

2. Trabalhos Relacionados

Diversos esforços têm sido realizados na área de jogos educativos voltados ao ensino de segurança da informação e criptografia, buscando utilizar estratégias lúdicas para promover a aprendizagem de maneira mais eficaz e envolvente. Esta seção apresenta uma seleção de iniciativas relevantes que, por meio de diferentes abordagens e públicos-alvo, exploram o potencial dos jogos e da gamificação no ensino de práticas seguras no ambiente digital. Esses trabalhos servem de referência para a concepção do *Cyber Defender*, cuja proposta visa ampliar as possibilidades educativas por meio de uma experiência imersiva e interativa.

O projeto CriptoData [Silva e Guarda 2019] foi desenvolvido com base no jogo digital educacional *Run Marco*, com o objetivo de ensinar conceitos de criptografia por meio da lógica de programação. O jogo trabalha a técnica de criptografia utilizando a Cifra de César, uma das técnicas mais clássicas e acessíveis de criptografia. A escolha dessa cifra se justifica por sua simplicidade conceitual, um vez que o jogo é voltado para o público da Educação Básica.

O CriptoLab [Guarda et al. 2018] por sua vez é um jogo educativo estruturado em cinco etapas, que explora a criptografia em um ambiente de computação desplugada associado ao pensamento computacional. As quatro primeiras fases seguem um mesmo padrão de atividades: resolução de questões de raciocínio lógico, decodificação de mensagens, busca por fichas e montagem de trechos de um código-fonte em formato desplugado. Essa divisão intencional do código visa estimular a habilidade de decomposição. A quinta e última etapa consiste na simulação da passagem por um labirinto impresso, consolidando os conhecimentos adquiridos ao longo das fases anteriores.

Diversas iniciativas têm explorado abordagens gamificadas e educativas para o ensino de conceitos de segurança da informação. Romão et al. (2024) apresenta um aplicativo gamificado voltado à geração de senhas fortes e memorizáveis. O estudo demonstrou que a aplicação obteve resultados satisfatórios tanto na memorização quanto na digitação das senhas, superando outros geradores convencionais.

Com foco no público idoso, o *Senior Safety* foi proposto como um aplicativo gamificado que incorpora elementos como pontuações, níveis e recompensas [Barbosa et al. 2025]. A ferramenta é composta por três módulos principais: o primeiro aborda o uso responsável da internet, o segundo trata da segurança no ambiente digital e o terceiro discute cuidados gerais a serem tomados. Ao longo desses módulos, são apresentados conceitos relacionados a fraudes, proteção de dados pessoais e utilização segura de redes sociais.

O jogo educativo *Alerta* [Júnior et al. 2024], foi desenvolvido com o objetivo de ensinar os usuários a identificar e-mails de *phishing*. Para isso, os autores criaram um conjunto de 36 e-mails, sendo 18 legítimos e 18 fraudulentos, utilizados durante as fases do jogo. Os jogadores deveriam discernir entre mensagens autênticas e maliciosas. Os resultados apontam que os participantes passaram a se sentir mais confiantes na identificação de tentativas de *phishing* após a experiência com o jogo.

No trabalho de Farias et al. (2019), foi desenvolvido o jogo *Self Protect*, direcionado ao ensino de conceitos de cibersegurança para crianças e adolescentes. A

iniciativa demonstrou impacto positivo na assimilação dos conteúdos abordados.

De maneira semelhante, Arachchilage e Cole (2011) propuseram um jogo para dispositivos móveis com foco no ensino de práticas seguras relacionadas ao *phishing*. Ambos os estudos evidenciaram resultados promissores, com os participantes apresentando melhor desempenho na identificação das técnicas comumente utilizadas em ataques de engenharia social. Esses trabalhos demonstram a eficácia de abordagens interativas e lúdicas no processo de ensino-aprendizagem de temas relacionados à cibersegurança, servindo como base e inspiração para a proposta deste artigo.

O jogo *Cyber Defender* se diferencia das abordagens anteriores ao oferecer uma experiência mais ampla e imersiva no ensino de cibersegurança. Com um ambiente explorável em visão *top-down* e desafios distribuídos em *minigames* apresentados por *NPCs*, o jogo integra diversos conceitos de forma contextualizada e interativa, proporcionando uma experiência educativa envolvente e dinâmica.

3. *Cyber Defender*: Projeto

O projeto do jogo *Cyber Defender* envolveu etapas desde a concepção até a implementação e testes. A primeira fase incluiu a criação de uma especificação detalhada, definindo o cenário como um escritório em uma visão *top-down*, na qual o jogador controla um personagem interagindo com diversos objetos e personagens. A modelagem do ambiente foi planejada com cuidado, assegurando a disposição lógica e funcional de elementos gráficos como chão, paredes, janelas, portas, mesas e equipamentos, garantindo uma experiência de jogo fluida e organizada.

O jogo é composto por *minigames*, os quais são apresentados por personagens não jogáveis (NPCs) que explicam o funcionamento de cada tarefa a ser realizada no jogo. A implementação do jogo foi realizada com a biblioteca *PyGame* em *Python*, que fornece funcionalidades para gráficos, animações, interações e controle de eventos, tornando-a ideal para o desenvolvimento eficiente e interativo do jogo educativo de segurança cibernética. Outras *engines* foram descartadas devido à alta curva de aprendizado, que poderia comprometer o cronograma de desenvolvimento do trabalho.

O projeto do *Cyber Defender* envolveu desde a concepção do cenário e das mecânicas até a implementação dos elementos gráficos, sonoros e narrativos. O jogo foi projetado com resolução Full HD (1920x1080) e taxa de atualização de 30 *FPS*, visando garantir uma experiência fluida e compatível com a maioria dos dispositivos.

Foram incorporados diversos elementos de gamificação conforme discutido por Feichas et al. (2021), incluindo um sistema de vidas e moedas. As moedas desempenham papel estratégico no jogo, permitindo que o jogador adquira dicas nos *minigames* e itens para a recuperação de vidas, promovendo decisões táticas e incentivando o engajamento contínuo.

A narrativa do jogo é um componente central da experiência. Cada personagem não jogável (NPC) possui uma personalidade definida e específica, contribuindo para uma ambientação mais rica e envolvente. Esses personagens assumem papéis relevantes na história, interagindo com o jogador de forma contextualizada e fortalecendo a imersão por meio de diálogos e instruções integradas ao enredo principal.

Além disso, foram adicionadas missões como desafios específicos que o jogador

deve completar para avançar no jogo. Essas missões estão diretamente conectadas à narrativa, reforçando o senso de progressão e propósito, e contribuindo simultaneamente para os objetivos lúdicos e educativos do projeto.

No aspecto visual, foram utilizados *assets* gráficos gratuitos provenientes do repositório *MuchoPixels* [MuchoPixels 2025], disponíveis na plataforma *Pixilart* [Pixilart 2025], além de elementos criados diretamente nessa mesma ferramenta. Essa escolha permitiu a composição de cenários organizados e visualmente agradáveis, com identidade coerente ao contexto do jogo.

Quanto à trilha sonora e efeitos, os recursos foram obtidos em plataformas como *Freesound.org* [FreeSound 2025] e *StockTune.com* [StockTune 2025], assegurando uma ambientação sonora que complementa a estética visual e favorece a imersão do jogador.

A consolidação de todos esses elementos — narrativos, visuais, sonoros e mecânicos — permitiu a criação de um ambiente de aprendizagem dinâmico e atrativo, capaz de envolver o jogador tanto cognitivamente quanto emocionalmente. O uso intencional da gamificação, aliado a uma narrativa coesa e a desafios progressivos, torna o *Cyber Defender* uma ferramenta promissora para o ensino de segurança da informação, especialmente por integrar conteúdos educativos em um contexto lúdico e interativo.

Na Seção seguinte, são detalhadas as fases do jogo, os elementos interativos presentes em cada cenário e a lógica de funcionamento dos *minigames*, além de apresentar as dinâmicas utilizadas para sustentar o engajamento do jogador ao longo da experiência.

4. *Cyber Defender*: Desenvolvimento

O *Cyber Defender* está disponível para *download* em duas versões, uma para *Windows* [1] e uma para *Linux* [2]. O jogo apresenta um cenário semelhante em suas três fases, sendo todas ambientadas em um escritório, um local escolhido para proporcionar familiaridade e contexto ao jogador, no sentido de criar um ambiente cotidiano e realista. Ao situar o jogo em um espaço comum, como um escritório, busca-se facilitar a identificação dos jogadores com a temática e tornar as situações de ciberataques mais tangíveis e compreensíveis. Além disso, o ambiente de escritório é frequentemente associado ao trabalho com tecnologia, o que reforça a relevância do aprendizado de segurança cibernética em um contexto profissional e cotidiano.

No entanto, embora o cenário mantenha essa base visual e estrutural, há uma evolução significativa ao longo das fases pois novos *NPCs* são gradualmente adicionados, aumentando a interação e complexidade do jogo. Esses *NPCs* desempenham papéis fundamentais na narrativa e nos desafios apresentados ao jogador, oferecendo instruções e dicas que enriquecem a jogabilidade e adicionam novos níveis de envolvimento.

Além do *NPC* "chefe" no canto superior direito, os outros *NPCs*, dispostos em seus respectivos computadores ao longo das fases, foram projetados com a função de explicar conceitos importantes relacionados ao tema de cada fase. Esses personagens servem como fontes de conhecimento, ajudando o jogador a entender tópicos de segurança cibernética que estão sendo abordados no jogo. O cenário da 1^a fase pode ser visualizado

[1] `https://drive.google.com/file/d/1mBeD6F1UToIy9UfkH-gp5u507vWN5AKo/`
[2] `https://drive.google.com/file/d/1O1FpH16DfRsqLjtmr9WzUaMBbTU1Dcvi/`

na Figura 1 na qual percebe-se no canto superior esquerdo o indicador de vida do personagem e a quantidade de moedas que o mesmo possui. Além disso, o cenário contém o chefe, localizado no canto superior direito, e demais objetos e *NPCs* na qual o usuário pode interagir.

Figura 1. Cenário da primeira fase do jogo *Cyber Defender*

Ao interagir com um NPC, é exibido um efeito visual que simula a digitação em uma máquina de escrever, acompanhado por um efeito sonoro correspondente. Essa combinação visa enriquecer a experiência do usuário, tornando a interação mais imersiva e envolvente. O sistema de vidas do jogo foi projetado para proporcionar um equilíbrio entre desafio e acessibilidade, incentivando o jogador a explorar o cenário e tomar decisões estratégicas para sua recuperação.

Para recuperar vidas, o jogador deve comprar itens chamados “petisco de cachorro ou gato” nas máquinas de venda automáticas espalhadas pelo cenário. Após adquirir o petisco, o jogador precisa interagir com o gato ou o cachorro presente no ambiente para que a vida seja restaurada. Este sistema não é imediatamente revelado ao jogador, oferecendo uma recompensa para aqueles que se dedicarem a explorar o ambiente

Em termos de conteúdo educativo, a primeira fase aborda o *phishing*, a segunda trata de *ransomware*, e a terceira fase é focada em ataques de *DDoS*. Esses *minigames* permitem que o jogador aplique na prática os conceitos aprendidos durante a fase principal, aumentando a imersão e o aprendizado de forma lúdica.

Em cada nível, o jogador deve realizar tarefas associadas ao tema central da fase, sendo que na fase de *phishing* o jogador deve identificar e-mails fraudulentos. Já no *minigame* de *ransonware*, o jogador deve buscar soluções para resolver o problema que o ataque gera. Por fim, a fase de *DDoS* tem como foco a proteção de servidores contra uma sobrecarga de requisições, ensinando o jogador estratégias para lidar com esse tipo de ataque cibernético.

Ao iniciar a primeira fase, um menu de instruções é apresentado ao jogador com o objetivo de familiarizar o mesmo com os comandos do jogo. Este menu pode ser visualizado na Figura 2 à esquerda e apresenta a primeira tarefa do jogo: dialogar com o chefe da empresa. Durante essa interação, o chefe introduz conceitos fundamentais sobre ataques de *phishing*, destacando que a missão da primeira fase consiste em avaliar

a autenticidade de e-mails suspeitos.

Cabe destacar que o chefe menciona a existência de uma lista de *e-mails* localizada em sua escrivaninha, sem, no entanto, identificar diretamente qual é. Com isso, o jogador é incentivado a explorar o ambiente do escritório, promovendo uma experiência investigativa que reforça o engajamento. Durante essa exploração, o jogador também é incentivado a interagir com outros funcionários (NPCs), os quais explicam o funcionamento do sistema de vidas e moedas, bem como o contexto organizacional do escritório.

Ao localizar sua escrivaninha, inicia-se o *minigame* da primeira fase. Neste desafio, o jogador deve analisar uma lista contendo 10 *e-mails* e identificar corretamente os 5 *e-mails* fraudulentos. Cada acerto — seja ao aceitar um *e-mail* legítimo ou rejeitar um *e-mail* falso — concede 10 moedas ao jogador. Por outro lado, decisões incorretas resultam na perda de uma vida. A Figura 2 apresenta o cenário do *minigame* correspondente à primeira fase.

Figura 2. Menu de instruções e *minigame* da primeira fase do jogodo jogo *Cyber Defender*

O *minigame* conta ainda com um indicador de tempo, que define um limite para a conclusão da tarefa. Caso o tempo se esgote ou todas as vidas sejam perdidas, o jogo é reiniciado. Se o jogador completar corretamente a tarefa antes do término do tempo, ele avança para a próxima fase, sendo instruído a retornar ao chefe para obter orientações adicionais.

Ao conversar novamente com o chefe, a resposta recebida varia conforme o desempenho do jogador na fase anterior, com base na quantidade de *e-mails* identificados corretamente. Essa adaptação de diálogo personaliza a experiência, promovendo maior imersão e incentivando o aprendizado.

A segunda fase inicia-se com uma nova interação com o chefe, que informa que a empresa está sob ataque de *ransomware*. O diálogo aborda os principais aspectos desse tipo de ameaça, incluindo formas de prevenção e mitigação. Dois novos *NPCs* são

inseridos no cenário e, ao interagir com eles, o jogador recebe orientações sobre práticas seguras, como a importância de *backups* e a verificação de arquivos suspeitos.

No *minigame* da segunda fase, o jogador é desafiado a completar duas tarefas. A primeira consiste na navegação por três labirintos sequenciais, com dificuldade crescente, a fim de localizar arquivos de *backup*. Esses labirintos são gerados dinamicamente por meio de um algoritmo de busca em largura (BFS), garantindo acessibilidade aos pontos de interesse e introduzindo variabilidade à jogabilidade.

Adicionalmente, a cada novo labirinto, o raio de visão do jogador é reduzido, aumentando o desafio e exigindo maior atenção e estratégia. A representação dos labirintos da segunda fase pode ser visualizado na Figura 3.

Na segunda tarefa desta fase, o jogador encontra arquivos criptografados que devem ser descriptografados por meio da resolução de anagramas compostos por termos relacionados à área de segurança da informação. Para auxiliar na resolução, o jogador pode adquirir dicas utilizando suas moedas acumuladas. Os termos utilizados, suas respectivas dicas e soluções são apresentados na Tabela 1.

Anagrama	**Dica**	**Palavra correta**
INGPHISH	Ataque com e-mails que parecem legítimos	Phishing
SODD	Ataque que sobrecarrega um serviço	DDoS
KEARCH	Perito em exploração de vulnerabilidades	Hacker
WALMERA	Software que causa danos no sistema	Malware
RAFWLILE	Barreira de proteção em redes	Firewall
VITRANUIS	Defesa contra ameaças digitais	Antivirus
KABUPC	Cópia de segurança de dados imporantes	Backup
TGRAIFCOPRIA	Técnica para proteger informações	Criptografia

Tabela 1. Anagramas, dicas e palavras utilizadas na segunda fase do jogo *Cyber Defender*

Finalizada essa fase, o jogador retorna ao chefe, cuja resposta é novamente adaptada de acordo com o desempenho, seja com parabenizações ou advertências, reforçando o caráter educativo e personalizado da experiência.

A terceira fase trata de ataques de negação de serviço distribuído (DDoS). No início desta fase, o chefe contextualiza a situação: a empresa está sob ataque e o jogador deve impedir que requisições maliciosas comprometam o sistema, preservando as requisições legítimas. Nesse diálogo, o chefe também explica os conceitos por trás do ataque e apresenta estratégias de defesa, como balanceamento de carga, uso de *firewalls* e mecanismos de *rate-limiting*.

NPCs adicionais fornecem explicações complementares sobre os impactos desses ataques e as ferramentas disponíveis para sua mitigação. O *minigame* desta fase, representado na Figura 3, é inspirado na dinâmica do jogo *Space Invaders*. O jogador deve interceptar requisições maliciosas e permitir a passagem das legítimas, controlando um personagem que dispara contra os alvos.

A atividade está dividida em três níveis, com progressão no volume e velocidade das requisições maliciosas. Para auxiliar o jogador, são disponibilizados quatro tipos de

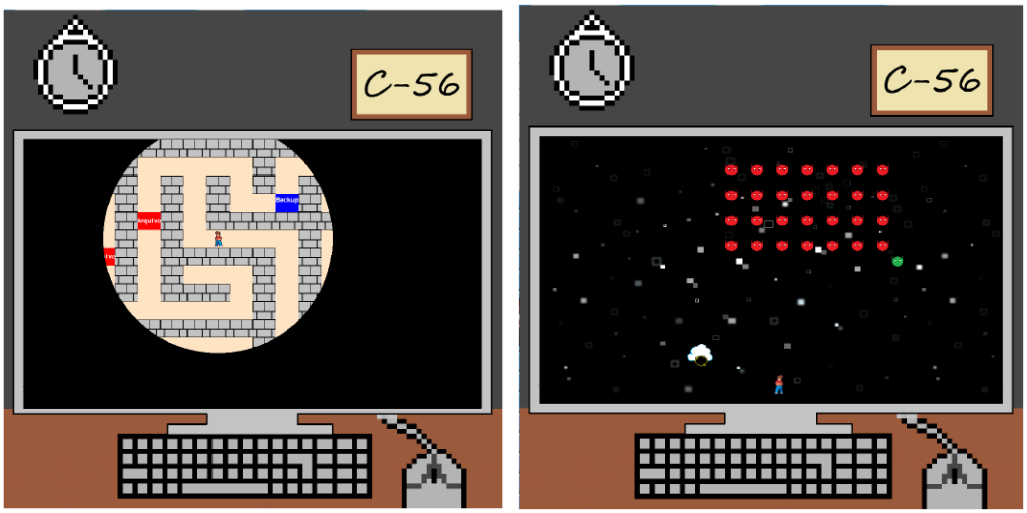

Figura 3. *Minigame* da segunda e terceira fase do jogo *Cyber Defender* - identificar requisições maliciosas

power ups, representando diferentes mecanismos de defesa contra *DDoS*. Os detalhes desses mecanismos encontram-se descritos na Tabela 2.

Power-up	**Ação**
CDN	Retorna os inimigos a posição inicial
Scrubbing tool	Remove uma parte dos inimigos
Firewall	Aumenta a taxa de disparos
Rate limiter	Diminui a velocidade dos inimigos

Tabela 2. Power-ups e ações da terceira fase do jogo *Cyber Defender*

No início do *minigame*, o jogador pode consultar os *power ups* disponíveis e adquirir novos itens com suas moedas, conforme necessário. A utilização estratégica desses recursos se torna fundamental à medida que o desafio se intensifica, contribuindo para a dinâmica do jogo e a aprendizagem dos conceitos de defesa digital.

5. Resultados e Discussões

A avaliação do jogo *Cyber Defender* foi conduzida por meio de quatro metodologias consolidadas na literatura: MEEGA+ [Petri et al. 2019], Instrumento de Avaliação da Qualidade de Jogos Educativos (IAQJEd) [Coutinho e Alves 2016], Pro-Avalia JS [de Oliveira et al. 2022] e Programa de Avaliação de Jogos Digitais Educacionais (PAJED) [Santos e Alves 2019]. Essas metodologias foram selecionadas por contemplarem critérios fundamentais à avaliação de jogos educacionais, como usabilidade, engajamento, experiência do usuário e impacto educacional.

O principal objetivo desta avaliação foi identificar os pontos fortes do jogo, bem como oportunidades de melhoria, de modo a assegurar que o *Cyber Defender* esteja alinhado às expectativas de interação, usabilidade e aprendizagem, típicas de jogos com fins educativos. Além disso, a avaliação buscou validar a adequação do jogo ao público-alvo e ao contexto pedagógico proposto.

O instrumento de coleta utilizado foi um formulário estruturado com 126 questões, das quais 123 estavam diretamente relacionadas aos critérios definidos pelas quatro metodologias de avaliação mencionadas. As três questões restantes tiveram caráter demográfico, voltadas à identificação da idade, gênero e curso de graduação dos participantes. O formulário também incluiu o Termo de Consentimento Livre e Esclarecido (TCLE), esclarecendo o caráter científico da pesquisa e garantindo o anonimato das respostas.

O formulário, juntamente com o link para acesso ao jogo, foi divulgado em plataformas digitais. Ao todo, 18 pessoas participaram da avaliação e preencheram o questionário. Com relação ao perfil dos respondentes, a média de idade foi de 22 anos, o que pode indicar familiaridade prévia com jogos digitais, considerando o perfil típico de jovens adultos que integram esse grupo etário. Em relação ao gênero, observou-se predominância do público masculino, com 16 participantes se identificando como homens e apenas 2 como mulheres.

No que se refere à formação acadêmica, a maioria dos participantes (10) cursava Ciência da Computação. As demais respostas foram distribuídas entre os cursos de Engenharia Civil (2), Engenharia Elétrica (1), Biomedicina (1), Bacharelado em Informática (1), Nutrição (1), Direito (1) e um participante que não declarou curso.

Essa diversidade pode contribuir para diferentes percepções sobre o jogo; no entanto, a baixa representatividade de estudantes de áreas fora das Ciências Exatas pode limitar a generalização dos resultados no contexto de públicos não especializados em tecnologia.

5.1. Resultados da Avaliação com o MEEGA+

A avaliação do jogo *Cyber Defender* por meio da metodologia MEEGA+ [Petri et al. 2019] teve como objetivo identificar a percepção dos jogadores em relação a diferentes dimensões da experiência com o jogo educacional. Essa metodologia utiliza uma escala *Likert* de cinco pontos, na qual 1 representa "discordo totalmente" e 5 representa "concordo totalmente" com as afirmações apresentadas aos participantes.

A MEEGA+ avalia nove componentes principais: Usabilidade, Confiança, Desafio, Satisfação, Interação Social, Diversão, Atenção Focada, Relevância e Aprendizagem Percebida. A Tabela 3 apresenta os resultados para cada um dos componentes avaliados. A seguir, são apresentados os conceitos avaliados em cada componente e os respectivos resultados obtidos na aplicação da metodologia com os 18 participantes da pesquisa.

A avaliação da usabilidade do jogo indicou que a navegação e os controles foram considerados acessíveis e intuitivos. Em relação à confiança, os participantes se sentiram capazes de avançar no conteúdo com base em suas próprias habilidades. O desafio foi avaliado como adequado, mantendo o engajamento sem gerar frustração, e a satisfação refletiu uma percepção positiva do aprendizado alcançado.

A interação social apresentou média baixa, devido ao foco em uma experiência individual mediada por NPCs, enquanto a diversão foi bem avaliada, destacando a experiência agradável proporcionada. A atenção focada foi considerada mediana, com sinais de imersão e dissociação temporal durante as atividades. A relevância do

Componente	Média
Usabilidade	4.1
Confiança	4.3
Desafio	3.8
Satisfação	4.1
Interação social	1.8
Diversão	4.6
Atenção focada	3.4
Relevância	4.2
Aprendizagem percebida	4.0

Tabela 3. Média de avaliação dos componentes do jogo *Cyber Defender* com o modelo MEEGA+ [Petri et al. 2019]

conteúdo foi reconhecida pelos jogadores, especialmente aqueles da área de tecnologia e segurança da informação, e a aprendizagem percebida confirmou ganhos concretos de conhecimento, validando a eficácia educacional do jogo.

5.2. Resultados da Avaliação com o PAJED

A avaliação do jogo *Cyber Defender* com base no Programa de Avaliação de Jogos Digitais Educacionais (PAJED) [Santos e Alves 2019] buscou mensurar seu potencial pedagógico por meio da análise de múltiplas dimensões do design instrucional e da experiência do usuário. O modelo PAJED é estruturado em oito categorias, cada uma voltada para aspectos fundamentais que contribuem para a eficácia do jogo no processo de ensino-aprendizagem. As categorias avaliadas foram: Feedback Imediato e Construtivo, Objetivos de Aprendizagem, Narrativa, Interatividade, Integração de Conceitos, Curva de Aprendizagem, Níveis Crescentes nos Desafios e Prática Colaborativa.

A metodologia utiliza a escala de Likert para a coleta das respostas, com posterior conversão dos valores para uma escala de 0 a 10, conforme definido pelo próprio modelo. Essa transformação possibilita o cálculo do Potencial de Aprendizagem (PA), indicador que sintetiza a qualidade educacional do jogo a partir dos escores obtidos em cada categoria. As médias das respostas para cada uma das categorias do PAJED podem ser vistas na Tabela 4.

Categoria	Média
Feedback imediato e construtivo	8.8
Objetivos de aprendizagem	8.7
Narrativa	8.4
Interatividade	7.3
Integração de conceitos	8.7
Curva de aprendizagem	8.0
Níveis crescente nos desafios	7.7
Prática colaborativa	6.4

Tabela 4. Média de avaliação dos componentes do jogo *Cyber Defender* com o modelo PAJED [Santos e Alves 2019]

No caso do *Cyber Defender*, o valor obtido para o PA foi de 80,7, o que, de acordo com a classificação do modelo PAJED, corresponde a um potencial de aprendizagem muito alto. Esse resultado evidencia que o jogo apresenta características bem desenvolvidas nos aspectos avaliados, destacando-se especialmente pelo fornecimento de feedbacks construtivos, pela clareza dos objetivos educacionais, pela narrativa envolvente, pela interatividade significativa e pela integração efetiva dos conceitos propostos.

Além disso, a avaliação indica que o jogo oferece uma progressão de desafios compatível com a curva de aprendizagem esperada, incentiva práticas colaborativas (mesmo que simuladas por NPCs) e proporciona uma experiência coerente e atrativa do ponto de vista educacional. Dessa forma, os dados obtidos com o PAJED reforçam a eficácia do *Cyber Defender* como uma ferramenta educacional, capaz de promover uma aprendizagem significativa por meio de uma proposta lúdica e bem estruturada.

5.3. Resultados da Avaliação com o IAQJEd

A avaliação do jogo *Cyber Defender* por meio do Instrumento de Avaliação da Qualidade de Jogos Educativos (IAQJeD) [Coutinho e Alves 2016] foi realizada considerando três dimensões principais: Usabilidade, Experiência de Usuário e Princípios de Aprendizagem. A dimensão de Usabilidade avalia aspectos como a facilidade de navegação, clareza das instruções e interação com a interface do jogo. A dimensão de Experiência de Usuário foca no engajamento e satisfação proporcionados ao jogador durante a execução das atividades propostas. Por fim, a dimensão de Princípios de Aprendizagem investiga como os fundamentos pedagógicos foram incorporados ao design do jogo, avaliando a coerência entre objetivos educacionais e as ações realizadas durante a jogabilidade.

As respostas foram coletadas utilizando uma escala do tipo *Likert* de cinco pontos. A pontuação final de cada dimensão foi obtida por meio da média das avaliações de cada questão correspondente. Os resultados obtidos foram:

- Usabilidade: média de 4,1 pontos, totalizando 25,0 pontos;
- Experiência de Usuário: média de 4,1 pontos, totalizando 24,8 pontos;
- Princípios de Aprendizagem: média de 3,9 pontos, totalizando 23,5 pontos.

A somatória das pontuações das três dimensões resultou em uma pontuação total de 73,3 pontos, em uma escala que varia entre 18 e 90 pontos. De acordo com os critérios de classificação estabelecidos pelo IAQJEd, essa pontuação corresponde à categoria de "Excelente qualidade para a finalidade educativa". Este resultado evidencia a capacidade do jogo *Cyber Defender* de promover uma experiência educativa eficaz, com boa usabilidade, engajamento significativo e sólida aplicação de princípios pedagógicos.

5.4. Resultados da Avaliação com o Pro-Avalia JS

A metodologia Pro-AvaliaJS [de Oliveira et al. 2022] foi aplicada com o objetivo de avaliar a qualidade do jogo *Cyber Defender* em diferentes dimensões relevantes para o contexto educacional. Este modelo considera aspectos essenciais como Usabilidade, Jogabilidade, Acessibilidade, Experiência do Jogador, Aspectos Pedagógicos e Conteúdo, oferecendo uma visão ampla e detalhada sobre a eficácia do jogo no processo de ensino-aprendizagem. A média das avaliações obtidas em cada uma dessas categorias é apresentada na Tabela 5.

Aspectos	Média
Usabilidade	4.4
Jogabilidade	4.6
Acessibilidade	4.4
Experiência do jogador	4.2
Aspectos pedagógicos	4.4
Conteúdo	4.5

Tabela 5. Média de avaliação dos componentes do jogo *Cyber Defender* com o modelo Pro-Avalia JS [de Oliveira et al. 2022]

Os resultados obtidos indicam que *Cyber Defender* apresenta desempenho elevado em todas as categorias analisadas, reforçando seu potencial como ferramenta educativa eficaz, acessível e pedagogicamente relevante.

Além disso os resultados indicam que o *Cyber Defender* apresenta desempenho consistente e satisfatório em todas as dimensões avaliadas pelo Pro-AvaliaJS. A predominância de médias superiores a 4,0 reforça o potencial do jogo como uma ferramenta eficaz de apoio ao ensino, combinando elementos lúdicos, pedagógicos e técnicos de maneira equilibrada.

5.5. Comparação dos resultados

A análise dos resultados revela diferentes percepções sobre aspectos essenciais do jogo Cyber Defender, como usabilidade, experiência do usuário/jogador e aspectos pedagógicos. Em termos de usabilidade, a avaliação geral do jogo mostra que ele é bem classificado em todas as metodologias. O jogo foi considerado fácil de usar, com boa acessibilidade e uma interface clara e intuitiva.

No entanto, os resultados indicam que o jogo teve um desempenho levemente melhor na Pro-AvaliaJS (Oliveira et al., 2022) (4,4), o que sugere que a avaliação da usabilidade neste modelo percebeu uma experiência mais fluida. Comparando com a pontuação obtida nas outras metodologias, MEEGA+ (Petri et al., 2019) e IAQJeD (Coutinho e Alves, 2016), ambas com 4,1, o jogo parece ser eficaz em atender aos requisitos de usabilidade, facilitando a interação e proporcionando uma navegação simples e direta.

A questão da experiência do usuário/jogador foi igualmente bem avaliada, com a Pro-AvaliaJS (Oliveira et al., 2022) (4,2) e a IAQJeD (Coutinho e Alves, 2016) (4,1) oferecendo boas notas para a forma como o jogo mantém o jogador engajado e confortável durante a experiência. A pontuação do PAJED (Santos, 2018), que obteve 8,0 em uma escala de 0 a 10, indica uma curva de aprendizagem positiva, sugerindo que o jogo permite que o jogador se familiarize com suas dinâmicas de maneira eficiente. Isso reflete a eficácia do jogo em proporcionar uma experiência onde os jogadores se sentem imersos, mas não sobrecarregados, com uma progressão adequada ao longo do tempo.

Em relação aos aspectos pedagógicos e à aprendizagem, os resultados mostram uma clara ênfase no impacto educacional do jogo. O jogo obteve uma pontuação mais alta na Pro-AvaliaJS (Oliveira et al., 2022) (4,4), o que indica que ele é bem projetado para atingir seus objetivos pedagógicos, proporcionando um aprendizado contínuo e

alinhado com o conteúdo educacional. A MEEGA+ (Petri et al., 2019) e a IAQJeD (Coutinho e Alves, 2016) apresentaram pontuações um pouco mais baixas (4,0 e 3,9, respectivamente), sugerindo que há margens para melhorar a integração do conteúdo educacional com a jogabilidade.

No entanto, em uma avaliação mais ampla, o PAJED (Santos, 2018) obteve uma pontuação impressionante de 8,7 (na escala de 0 a 10), o que aponta que o jogo é eficaz em integrar conceitos e promover a aprendizagem, focando na transferência do conhecimento de forma clara e eficaz.

No que se refere à interação social, os resultados indicam uma deficiência nesse aspecto dentro do jogo, com pontuações de 1,8 na MEEGA+ (Petri et al., 2019) e 6,4 no PAJED (Santos, 2018). Esses valores sugerem que a experiência social proporcionada pelo jogo é limitada, possivelmente impactando o engajamento e a colaboração entre os jogadores. Esses resultados indicam que, em termos de usabilidade, o jogo oferece uma interface amigável e fácil de navegar, enquanto a experiência do usuário e a curva de aprendizagem são igualmente bem recebidas, mostrando que os jogadores conseguem se adaptar rapidamente ao jogo.

Além disso, os aspectos pedagógicos estão bem alinhados com os objetivos de aprendizagem, mas ainda podem ser aprimorados em termos de integração e aprofundamento do conteúdo. Uma possível melhoria seria o fortalecimento da interação social dentro do jogo, visto que esse aspecto apresentou pontuações mais baixas, sugerindo a necessidade de mecânicas que incentivem a colaboração ou a competição saudável entre os jogadores. Com isso, o jogo se apresenta como uma ferramenta eficiente para promover o aprendizado, com destaque para sua usabilidade e o impacto positivo na experiência do jogador.

6. Conclusões e Trabalhos Futuros

Este trabalho teve como objetivo o projeto e desenvolvimento do jogo educativo *Cyber Defender*, voltado ao ensino de conceitos fundamentais de segurança digital. Para validar a eficácia do jogo como ferramenta educacional, foram aplicadas quatro metodologias distintas de avaliação de jogos educativos: MEEGA+ [Petri et al. 2019], IAQJEd [Coutinho e Alves 2016], Pro-Avalia JS [de Oliveira et al. 2022] e PAJED [Santos e Alves 2019]. Essas metodologias permitiram uma análise abrangente de aspectos como usabilidade, engajamento, experiência do usuário e impacto educacional.

Os resultados obtidos nas avaliações indicam que o *Cyber Defender* apresenta uma narrativa bem estruturada, jogabilidade satisfatória e uma abordagem eficaz no tratamento dos conteúdos educativos propostos. Tais características reforçam o potencial do jogo como uma ferramenta de apoio ao processo de ensino-aprendizagem, especialmente no contexto da segurança digital.

Como trabalhos futuros, propõe-se a inclusão de elementos que ampliem a interação social dentro do jogo, como modos cooperativos ou competitivos, além do ajuste dinâmico do nível de desafio, com o intuito de manter o engajamento contínuo dos jogadores. Também se considera relevante expandir o público-alvo, adaptando o conteúdo e as mecânicas para diferentes faixas etárias e contextos culturais, bem como realizar novas avaliações que permitam acompanhar o impacto das melhorias implementadas.

Conclui-se que o uso de jogos educativos, como o *Cyber Defender*, pode contribuir significativamente para o aumento do engajamento dos alunos, promovendo a motivação para a aprendizagem, ao mesmo tempo em que educa e previne problemas relacionados à segurança digital no ambiente online.

Agradecimentos

Agradecimentos ao Manna_Team, à Fundação Araucária de Apoio ao Desenvolvimento Científico e Tecnológico do Estado do Paraná (FA) e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) – Brasil (Processo nº 421548/2022-3) pelo apoio.

Referências

Aljohani, M., Alruqi, M., Alboqomi, O., e Alqahtani, A. (2020). An experimental study to understand how users choose password. In *Proceedings of the 4th International Conference on Future Networks and Distributed Systems*, pages 1–5.

Arachchilage, N. A. G. e Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". In *International conference on information society (i-society 2011)*, pages 485–489. IEEE.

Barbosa, B. R., Morais, A. G., de Sousa Morais, M. H. B., e Júnior, J. C. L. (2025). Senior safety: uma aplicação móvel de educação em segurança digital para pessoas idosas usando gamificação. *Cadernos Cajuína*, 10(1):e728–e728.

Coutinho, I. d. J. e Alves, L. (2016). Instrumento de avaliação da qualidade de jogos digitais com finalidade educativa (iaqjed). In *Anais do XXXIX Congresso Brasileiro de Ciências da Comunicação*, pages 1–16.

de Oliveira, R. N., Belarmino, G. D., Minholi, F. S., Rodriguez, C., Goya, D., e Rocha, R. V. (2022). Pro-avaliajs: Protocolo para planejamento e execução da avaliação da reação e aprendizagem de jogos sérios. In *Anais do XXXIII Simpósio Brasileiro de Informática na Educação*, pages 517–527. SBC.

Farias, F. L. d. O., de Medeiros, N. A. A., da Rocha, S. L., de Medeiros, D. F., da Nóbrega, E. C., Burlamaqui, A., e Madeira, C. (2019). Self protect: Um jogo para auxílio no ensino de conceitos relacionados a segurança na internet para crianças e adolescentes. In *Anais do Workshop de Informática na Escola*, volume 25, pages 246–255.

Feichas, F. A., Seabra, R. D., e de Souza, A. D. (2021). Gamificação no ensino superior em ciência da computação: Uma revisão sistemática da literatura. *Revista Novas Tecnologias na Educação*, 19(1):443–452.

FreeSound (2025). Freesound - find any sound you like. `https://freesound.org/`. Accessado em janeiro 2025.

Gris, G. e Souza, S. R. d. (2016). Digital educational games and model of network relations: development and evaluating of the physical prototype of korsan game. *Perspectivas em análise do comportamento*, 7(1):114–132.

Guarda, G., Silva, D., e Goulart, I. (2018). Criptolab: Um game baseado em computação desplugada e criptografia. In *Workshop sobre Educação em Computação (WEI), XXVI*, pages 49–59.

Júnior, J. F., Henklain, M., Lobo, F., e Feitosa, E. (2024). Avaliação da eficiência de jogo educativo para o ensino do comportamento de distinguir e-mails legítimos de tentativas de phishing. In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 219–232, Porto Alegre, RS, Brasil. SBC.

Kaspersky (2024). Kaspersky security bulletin 2024. statistics. `https://securelist.com/ksb-2024-statistics/114795/`. Accessado em março 2025.

Lin, X., Araujo, F., Taylor, T., Jang, J., e Polakis, J. (2023). Fashion faux pas: Implicit stylistic fingerprints for bypassing browsers' anti-fingerprinting defenses. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 987–1004. IEEE.

MuchoPixels (2025). Muchopixels - pixel art. `https://www.muchopixels.com/`. Accessado em janeiro 2025.

Panosso, M. G., Souza, S. R. d., e Haydu, V. B. (2015). Características atribuídas a jogos educativos: uma interpretação analítico-comportamental. *Psicologia Escolar e Educacional*, 19:233–242.

Paschoal, L. N., Valle, P. H. D., e Melo, S. M. (2020). Um estudo terciário sobre o ensino de computaçao no brasil. *Revista Novas Tecnologias na Educação*, 18(1).

Petri, G., Gresse von Wangenheim, C., e 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(3).

Pixilart (2025). Pixilart - free online art community and pixel art tool. `https://www.pixilart.com/`. Accessado em janeiro 2025.

Romão, H., Henklain, M., Lobo, F., e Feitosa, E. (2024). Construção e teste de app gamificado gerador de senhas fortes e memoráveis: Um estudo exploratório em cibersegurança. In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 256–269, Porto Alegre, RS, Brasil. SBC.

Santos, W. e Alves, L. R. G. (2019). Pajed: Um programa de avaliaçao de jogos digitais educacionais. *Anais do Seminário de Jogos Eletrônicos, Educação e Comunicação*.

Silva, D. J. e Guarda, G. (2019). Criptodata: Ensino de criptografia via computação desplugada. In *Anais dos Workshops do Congresso Brasileiro de Informática na Educação*, volume 8, page 248.

StockTune (2025). Stocktune: Free stock music, endless possibilities. `https://stocktune.com/`. Accessado em janeiro 2025.

Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., e Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE access*, 10:39325–39343.

Tsutsumi, M. M. A., Goulart, P. R. K., Júnior, M. D. S., Haydu, V. B., e de Oliveira Jimenéz, É. L. (2020). Avaliação de jogos educativos no ensino de conteúdos acadêmicos: Uma revisão sistemática da literatura. *Revista Portuguesa de Educação*, 33(1):38–55.