



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

CyberWar: Um Jogo Digital Como Ferramenta de Ensino sobre Ataques Cibernéticos *

CyberWar: A Digital Games as a Teaching Tool for Cyber Attacks

Pedro Henrique dos Santos¹
Samuel Oliveira Guedes²
Wesley Dias Maciel³

Resumo

O aumento da digitalização da sociedade tem ampliado a exposição de usuários a ataques cibernéticos, revelando a limitação dos métodos tradicionais de ensino em cibersegurança, que geralmente não despertam engajamento efetivo. Neste trabalho, foi desenvolvido o *CyberWar*, um jogo digital como ferramenta didática para promover aprendizado interativo e envolvente sobre cibersegurança. O objetivo do estudo foi desenvolver um jogo educativo que ensina conceitos de segurança digital, com foco em ataques do tipo *phishing* e *man-in-the-middle*. O projeto foi implementado em ambiente 3D isométrico com minijogos que simulam situações reais, permitindo ao usuário identificar ameaças e aplicar boas práticas de proteção. A metodologia adotada foi baseada no *framework Scrum*. O trabalho foi avaliado através da aplicação de questionários pré e pós-jogo para mensurar o conhecimento sobre cibersegurança adquirido pelos usuários. Os resultados indicaram um aumento significativo no entendimento sobre cibersegurança dos participantes, especialmente em temas como engenharia social e identificação de tentativas de fraude. Como conclusão, foi observado que jogos digitais, quando bem estruturados, ajudam transmitir conteúdos técnicos. Além disso, o *CyberWar* contribuiu para a formação de uma cultura de segurança digital e para a redução de comportamentos de risco em ambientes pessoais e corporativos.

Palavras-chave: Cibersegurança. Jogos Digitais. Gamificação. Ataques Cibernéticos. Ensino Interativo.

*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais como pré-requisito para obtenção do título de Bacharel em Sistemas de Informação.

¹Aluno do Programa de Graduação em Ciência da Computação, Brasil – pedrohenriquesantos0303@gmail.com.

²Aluno do Programa de Graduação em Ciência da Computação, Brasil – samuel150204@gmail.com.

³Professor do Programa de Graduação em Ciência da Computação, Brasil – wesleymaciel@pucminas.br.

Abstract

The increasing digitalization of society has heightened users' exposure to cyberattacks, revealing the limitations of traditional cybersecurity education methods, which often fail to foster effective engagement. In this work, we present *CyberWar*, a digital game designed as an educational tool to promote interactive and immersive learning. The study aimed to develop a game that teaches digital security concepts, focusing on phishing and man-in-the-middle attacks. The game was implemented in an isometric 3D environment and includes minigames that simulate real-world scenarios, enabling users to identify threats and apply best protection practices. The development methodology followed the Scrum framework. We evaluated the game using pre- and post-game questionnaires to assess users' cybersecurity knowledge acquisition. The results showed a significant improvement in participants' understanding of cybersecurity, particularly in areas such as social engineering and phishing recognition. We conclude that well-designed digital games are effective tools for delivering technical content in an accessible way. Furthermore, *CyberWar* has contributed to fostering a culture of digital security and reducing risky behavior in both personal and corporate environments.

Keywords: Cybersecurity. Digital Games. Gamification. Cyberattacks. Interactive Learning

1. INTRODUÇÃO

A intensificação da transformação digital nas últimas décadas alterou as formas de transmissão, armazenamento e uso de dados, ampliando a dependência de serviços *online* e expondo usuários e organizações a um cenário crescente de ameaças cibernéticas. No Brasil, entre 2019 e 2023, as transações bancárias por smartphones aumentaram em 251%, totalizando 130,7 bilhões de operações em 2023, sendo 79% realizadas por meio de canais digitais, como aplicativos e *internet banking* (FEBRABAN, 2024). Esse avanço tecnológico, embora represente melhorias em acessibilidade e eficiência, também impõe desafios à segurança da informação, principalmente devido à falta de conhecimento técnico por parte dos usuários sobre práticas básicas de proteção. Esse cenário pode ser analisado sob duas perspectivas interdependentes: a corporativa e a individual. No contexto organizacional, empresas que lidam com dados sensíveis tornaram-se alvos frequentes de cibercriminosos, como no caso ocorrido em dezembro de 2020, quando uma falha no sistema do Ministério da Saúde expôs dados de 243 milhões de brasileiros. A causa foi a exposição indevida de credenciais administrativas, evidenciando fragilidades nos mecanismos de proteção utilizados (G1, 2020). No âmbito individual, a baixa familiaridade com medidas de segurança digital continua sendo explorada por técnicas de engenharia social, que utilizam manipulação psicológica para obter acesso a dados sensíveis. Estima-se que, em 2024, os crimes cibernéticos tenham gerado prejuízos globais de US\$9,5 trilhões, com projeções de atingir US\$10,5 trilhões até 2025 (SENHASEGURA, 2024). Diante do aumento de fraudes digitais, roubos de identidade e ataques cibernéticos, torna-se essencial promover iniciativas voltadas à conscientização sobre segurança digital, abordando a proteção de dados não apenas como questão técnica, mas como parte fundamental da vida digital contemporânea.

Por meio disso, a cibersegurança enfrenta obstáculos críticos, especialmente relacionados ao fator humano e à carência de estratégias eficazes de conscientização. A desinformação sobre ameaças digitais e a ausência de hábitos seguros tornam os usuários alvos recorrentes de ataques cibernéticos. No ambiente corporativo, essa vulnerabilidade se agrava devido a práticas como o uso de senhas fracas, o compartilhamento de credenciais e a falta de atenção na verificação de *emails* suspeitos, que podem comprometer os sistemas mesmo em empresas que investem em soluções de segurança. Muitos desses incidentes derivam de falhas humanas evitáveis, o que confirma a fragilidade do fator humano como elo mais vulnerável na cadeia da segurança da informação (SANGWAN, 2024). Paralelamente, a maioria das iniciativas educacionais em cibersegurança continua fundamentada em métodos tradicionais, como palestras e manuais, os quais mostraram-se insuficientes para engajar os usuários ou promover retenção significativa do conteúdo (SREEHARI et al, 2023). Diante disso, essa limitação ressalta a urgência por abordagens

mais integrativas e acessíveis, capazes de promover aprendizado contínuo e mudanças concretas no comportamento digital e na cultura organizacional. Diante desse cenário, emergiu uma questão central: de que forma os jogos digitais poderiam contribuir para a conscientização em segurança cibernética?

Dessa forma, o aumento dos ataques cibernéticos compromete seriamente a segurança de dados pessoais e corporativos, muitas vezes devido ao despreparo dos usuários diante das ameaças digitais. Diante disso, é fundamental desenvolver estratégias que tornem o aprendizado em cibersegurança mais acessível, atrativo e adequado a diferentes perfis. Um paralelo útil pode ser traçado com o ensino de Física, que enfrenta dificuldades similares por seu caráter abstrato e pela falta de recursos visuais e práticos (KUO et al, 2024). A cibersegurança enfrenta o mesmo desafio, já que costuma ser ensinada de forma teórica, por meio de palestras, cursos expositivos e textos extensos, pouco eficazes para quem não tem formação técnica. Embora essas abordagens tenham valor, sua limitação em engajar e garantir retenção de conteúdo evidencia a necessidade de métodos mais eficientes. Nesse cenário, os jogos digitais surgem como alternativa promissora, unindo prática e engajamento. Com a gamificação, usuários podem simular ataques e aplicar defesas em ambientes seguros, facilitando a compreensão de conceitos complexos. Essa abordagem transforma conteúdos abstratos em experiências concretas, incentiva a participação ativa e torna o aprendizado mais intuitivo, eficaz e alinhado às demandas atuais da educação digital (SANGWAN, 2024).

Diante disso, este estudo teve como objetivo desenvolver um jogo digital interativo para promover a conscientização sobre ataques cibernéticos, oferecendo uma alternativa mais acessível, envolvente e eficaz em comparação aos métodos tradicionais, como palestras e treinamentos teóricos, que muitas vezes não engajam nem garantem retenção de conteúdo. A proposta foi voltada tanto a usuários comuns quanto a profissionais de ambientes corporativos, onde a segurança da informação é fundamental. Com uma abordagem lúdica, o jogo simula situações reais de ameaças como *phishing* e *man-in-the-middle (MITM)*, permitindo aos usuários aprender, de forma prática, a identificar e prevenir ataques. Para isso, foram definidos como objetivos específicos a análise dos principais ataques cibernéticos, a construção de uma narrativa gamificada, o *design* de minijogos com mecânicas baseadas em ataques reais e a avaliação do impacto da ferramenta sobre o conhecimento dos participantes. A partir dessas diretrizes, foi criado o *CyberWar*, um jogo em ambiente 3D isométrico fundamentado na aprendizagem baseada em jogos digitais (*Digital Game Based Learning - DGBL*), que expõe os usuários a desafios inspirados no cotidiano digital. A metodologia adotada seguiu uma abordagem mista, com aplicação de questionários antes e depois da interação com o jogo, permitindo mensurar a

evolução do aprendizado. Como principal resultado, observou-se um aumento significativo no índice de acertos em questões sobre cibersegurança, além de todos os participantes relatarem maior confiança para identificar tentativas de *phishing* e compreender estratégias de engenharia social. Assim, o trabalho desenvolvido buscou, como ferramenta educativa, contribuir para o fortalecimento da cultura de segurança digital, promovendo aprendizado ativo e redução de comportamentos de risco tanto no uso cotidiano quanto em ambientes corporativos.

Este trabalho está organizado em sete partes principais. A seção 2 apresenta o referencial teórico que aborda métodos de ensino, abordagens de ensino em jogos digitais e conceitos de cibersegurança. A seção 3 demonstra os trabalhos relacionados que analisam iniciativas similares ao presente trabalho. Na seção 4, o desenvolvimento detalha a criação do jogo *CyberWar*, com seus *minigames*. Na seção 5 a metodologia explica a pesquisa mista com questionários pré e pós-teste, além das tecnologias utilizadas. Na seção 6 é abordado os resultados e discussões da pesquisa obtidos pelos questionários. Por fim, na seção 7 é apresentada a conclusão do presente trabalho.

2. REFERENCIAL TEÓRICO / FUNDAMENTAÇÃO TEÓRICA

Este referencial teórico tem como objetivo apresentar os principais conceitos que embasam a proposta deste trabalho, abordando métodos de ensino modernos, o uso de jogos digitais como estratégia educacional e fundamentos sobre cibersegurança. A seguir, são exploradas as bases teóricas que sustentam a aplicação da gamificação no ensino de temas relacionados à segurança digital.

2.1. Métodos de Ensino

A educação tem passado por grandes transformações nas últimas décadas, principalmente devido à evolução tecnológica e às novas descobertas sobre o funcionamento do aprendizado humano. O modelo tradicional de ensino, baseado na transmissão passiva de conhecimento pelo professor e na memorização por parte do aluno, tem demonstrado diversas limitações no processo de aprendizagem. Embora tenha sido a base da educação por séculos, esse método muitas vezes não consegue engajar os estudantes de forma significativa, levando a um aprendizado superficial e pouco duradouro (ZHAO et al, 2022). Por outro lado, os métodos modernos de ensino, como a aprendizagem baseada em jogos, têm se mostrado mais eficazes em engajar os estudantes e melhorar sua motivação. Um estudo realizado comparou o ensino tradicional com a *DGBL* em cursos de ciência da computação, utilizando jogos criados por professores (FERNANDEZ et al, 2021). Os resultados demonstraram que, embora ambos os métodos fossem igualmente eficazes na aquisição de conhecimento, a *DGBL* foi significativamente superior em aumentar a motivação dos

alunos, com a maioria preferindo essa abordagem em relação ao ensino tradicional. Essas metodologias modernas enfatizam a resolução de problemas reais e o contato direto com o domínio de estudo, estimulando o aprendizado através da experiência. O aprendizado ativo, promovido por essas abordagens, incentiva a criatividade, o pensamento crítico e a retenção de conhecimento a longo prazo, comprovando que estratégias interativas, como jogos educacionais, são mais eficientes do que os modelos tradicionais de ensino.

2.2. Abordagens de ensino com Jogos Digitais

Os jogos digitais têm sido amplamente utilizados como ferramentas educacionais, e diferentes abordagens foram desenvolvidas para integrar esses jogos ao aprendizado. Entre as principais estratégias, destacam-se a *DGBL*, os jogos sérios e a gamificação.

A aprendizagem baseada em jogos digitais envolve o uso de jogos como meio de ensino, proporcionando uma experiência interativa e imersiva (SREEHARI et al., 2023). Nessa abordagem, os conceitos educacionais são incorporados diretamente à mecânica do jogo, permitindo que os alunos aprendam ao resolver desafios e explorar cenários. A *DGBL* é eficaz porque transforma o aprendizado em uma experiência envolvente e motivadora, adaptando-se ao ritmo e às necessidades individuais dos alunos.

Outra abordagem relevante é a dos jogos sérios, que são desenvolvidos com um propósito educacional explícito, indo além do mero entretenimento. Esses jogos são projetados para ensinar conteúdos específicos, treinar habilidades ou simular situações do mundo real (SANTIAGO et al, 2023). Diferentemente dos jogos tradicionais, que priorizam a diversão, os jogos sérios utilizam mecânicas de jogo para abordar temas complexos, como segurança cibernética, medicina e direito.

Por fim, a gamificação é uma abordagem que aplica elementos de *design* de jogos em contextos não relacionados a jogos, com o objetivo de aumentar o engajamento e a motivação dos participantes (SANTIAGO et al, 2023). Essa técnica utiliza componentes típicos dos jogos, como pontos, medalhas, *ranking* e desafios, para incentivar a aprendizagem e a participação ativa dos alunos. A gamificação tem o potencial de tornar atividades tradicionalmente monótonas mais estimulantes, pois estimula a adoção e a manutenção de determinados comportamentos, motivando o usuário a cumprir tarefas claras, significativas, desafiadoras e recompensadoras (AFONSO et al , 2021).

Portanto, o jogo desenvolvido se enquadra na categoria de *DGBL*, pois utiliza técnicas interativas para ensinar conceitos essenciais de cibersegurança de maneira envolvente e prática. O jogo oferece um ambiente simulado onde os jogadores podem experimentar ataques cibernéticos e aprender a identificá-los, fortalecendo sua capacidade de reagir a ameaças reais.

2.3. Cibersegurança

A cibersegurança, também conhecida como segurança cibernética, refere-se aos métodos e tecnologias adotadas pelo mercado a fim de proteger principalmente sistemas, redes, dispositivos e dados contra ataques digitais, acessos não autorizados, danos ou roubo de informação (NASUTION et al, 2024). Seu objetivo principal é assegurar a confidencialidade, integridade e disponibilidade dos dados no ambiente digital. Diante disso, a cibersegurança está relacionada com o conhecimento sobre os ataques cibernéticos e engenharia social, tendo em vista que para traçar estratégias de combate sobre ações ilegais via *internet* é preciso conhecer como são realizadas as práticas de roubo de informação.

2.4. Ataques Cibernéticos

Os ataques cibernéticos são ações maliciosas conduzidas por indivíduos ou grupos com o objetivo de comprometer a segurança digital de sistemas e redes. Esses ataques podem visar o roubo de dados confidenciais, a interrupção de serviços ou a danificação de infraestruturas tecnológicas. Para alcançar esses objetivos, os cibercriminosos exploram vulnerabilidades e empregam diversas técnicas para obter acesso não autorizado aos sistemas-alvo.

Uma dessas técnicas é a engenharia social, que consiste na manipulação psicológica das vítimas para explorar a confiança humana e obter dados sensíveis ou acesso a sistemas protegidos. Esse conceito está diretamente relacionado à exploração de erros humanos (NASUTION et al, 2024), frequentemente cometidos no ambiente de trabalho. Golpes como ligações telefônicas fraudulentas, mensagens enganosas e interações presenciais com funcionários são exemplos de estratégias utilizadas para extrair dados confidenciais.

Outra abordagem amplamente empregada é o *man-in-the-middle*, um ataque em que o invasor intercepta a comunicação entre dois dispositivos legítimos na rede. Para isso, o atacante modifica o endereço *Media Access Control (MAC)* de cada dispositivo para que os dados trafeguem por ele, tornando-se um intermediário não autorizado na comunicação (SAED et al, 2024). Esse tipo de ataque possibilita a captura, modificação ou redirecionamento de informação, podendo resultar no roubo de credenciais bancárias e dados pessoais. Para mitigar este risco, recomenda-se o uso de criptografia ponta a ponta, autenticação multifator e certificados digitais que garantam a legitimidade de sites e serviços. Além disso, o uso de redes *Wi-Fi* públicas deve ser evitado ou protegido por meio de *Virtual Private Network (VPN)* , reduzindo a possibilidade de interceptação de dados.

Por fim, o *phishing* é uma técnica que busca enganar os usuários para que revelem dados confidenciais, como senhas, números de cartão de crédito e credenciais de acesso. Esse tipo de

ataque ocorre principalmente por meio de *email*, mensagens ou sites fraudulentos que imitam serviços legítimos, induzindo a vítima a fornecer dados sigilosos sem perceber a fraude. Muitas vezes, *links* modificados direcionam o usuário a páginas falsas ou instalam arquivos maliciosos ao serem clicados, comprometendo redes corporativas (NASUTION et al, 2024). Para evitar tais ataques, é essencial investir em treinamentos de conscientização, implementar filtros avançados de *emails* para bloquear mensagens suspeitas e verificar a autenticidade dos remetentes antes de clicar em *links* ou baixar anexos. Além disso, a adoção da autenticação multifator acrescenta uma camada extra de segurança, dificultando acessos indevidos.

3. TRABALHOS RELACIONADOS

Com base no contexto apresentado, há diversas iniciativas que se baseiam em criar jogos que de forma lúdica ensinam as pessoas e conseguem reter a atenção das mesmas. Nos próximos parágrafos serão apresentados alguns trabalhos, que assim como este, visa trazer conhecimento de uma forma diferente das utilizadas comumente.

Um dos trabalhos relevantes neste contexto é o *CyberLearn2D*, um jogo educacional desenvolvido com base na metodologia de aprendizagem baseada em jogos digitais, cujo principal objetivo é ensinar conceitos fundamentais de cibersegurança por meio de desafios práticos e interativos (PIKI et al, 2024). O jogo foi implementado utilizando *Python* em ambiente *Linux Ubuntu* e aborda seis temas centrais de ameaças digitais: senhas, *spam*, *phishing*, vírus, *malware* e *ransomware*. Durante o jogo, os usuários enfrentam desafios que simulam situações reais, sendo incentivados a reconhecer ameaças, tomar decisões estratégicas e aplicar medidas de segurança dentro de um ambiente virtual. Uma avaliação piloto com 20 participantes de diferentes faixas etárias indicou que o *CyberLearn2D* foi eficaz em aumentar a conscientização sobre boas práticas de segurança digital, especialmente entre usuários com pouca familiaridade prévia com o tema. Entretanto, o projeto apresentou algumas limitações. A ausência de avaliações em larga escala limita a generalização dos resultados, e a necessidade de atualização contínua dos conteúdos, frente à rápida evolução das ameaças cibernéticas, representa um desafio significativo para a sustentabilidade do jogo. Diante disso, o *CyberLearn2D* se concentra em *quizzes* e respostas rápidas, sendo que, o trabalho aqui proposto, o *CyberWar*, também se baseia na *DGBL* para promover a educação em cibersegurança, mas adota uma abordagem mais narrativa e imersiva. Enquanto o *CyberLearn2D* organiza o conteúdo em níveis temáticos com foco em tarefas práticas isoladas, o *CyberWar* insere o jogador em uma história contínua baseada em simular as ameaças atuais. Além disso, o *CyberWar* valoriza o desenvolvimento de habilidades práticas ao integrar *minigames* que simulam cenários reais, proporcionando uma experiência contextualizada e alinhada com a evolução dos métodos de ataque modernos.

Outro trabalho relevante, o *CyberSecApp* é um aplicativo gamificado voltado para o ensino de conceitos básicos de cibersegurança de forma interativa e acessível. A plataforma foi estruturada em três níveis de atividades: *quizzes*, um jogo baseado no "Jogo da Forca" e uma narrativa adaptada do conto "Chapeuzinho Vermelho" para o contexto da segurança digital (CRIOLLO-C et al, 2024) . Sua eficácia foi avaliada com 60 estudantes universitários de engenharia, sendo que foi utilizado ferramentas para medir a usabilidade e para analisar a carga mental. Os resultados indicaram uma melhoria de 14,47% no desempenho em testes de conhecimento após o uso do aplicativo, além de elevados níveis de satisfação com a interface e percepção de baixa carga cognitiva. No entanto, o estudo apresentou limitações, como a ausência de um grupo de controle para comparação com métodos tradicionais, a restrição da amostra ao contexto acadêmico e a indicação de usuários quanto à necessidade de novas funcionalidades e conteúdos mais avançados. Comparando o *CyberSecApp* ao presente trabalho observam-se semelhanças e diferenças relevantes. Ambos os projetos adotam a gamificação como estratégia de ensino e utilizaram a metodologia *Scrum* (SCHWABER;SUTHERLAND,2020) para o desenvolvimento ágil. Porém, o *CyberSecApp* concentra-se na introdução conceitual à segurança digital, utilizando mecânicas simples e narrativas lúdicas voltadas para iniciantes. Em contraste, o *CyberWar* oferece uma experiência com conceitos mais avançados e realistas, na qual os jogadores enfrentam ataques cibernéticos simulados e aplicam estratégias práticas de proteção. Além disso, enquanto o *CyberSecApp* foi aplicado exclusivamente em um contexto acadêmico, o *CyberWar* foi desenvolvido para atender tanto usuários individuais quanto profissionais de ambientes corporativos.

Por fim, o *NetDefense* é um jogo educacional que busca ensinar conceitos básicos de cibersegurança a estudantes do ensino fundamental e médio, utilizando a dinâmica de jogos do gênero *tower defense*. Desenvolvido em *Unity* (UNITY TECHNOLOGIES, 2025) e disponibilizado em *Unity WebGL* (UNITY TECHNOLOGIES, 2025) para navegadores, o jogo simula a defesa de redes virtuais, onde os jogadores devem posicionar e configurar roteadores para bloquear pacotes maliciosos e permitir o tráfego legítimo (TOLEDO et al, 2024). Para tornar a experiência mais envolvente, foram implementados modelos temáticos baseados em setores da economia, conectando os desafios de segurança a contextos práticos do mundo real. Em sua avaliação, realizada com professores, os resultados mostraram um aumento significativo no entendimento sobre pacotes de dados, *firewalls* e *honeypots*. No entanto, o estudo apresentou algumas limitações sobre apenas se concentrar em aspectos técnicos da segurança, como a configuração de redes, sem abordar ameaças sociais e comportamentais, como engenharia social e privacidade *online*. O presente trabalho compartilha o propósito do *NetDefense* ao utilizar a gamificação para ensinar

cibersegurança de maneira interativa. No entanto, há diferenças importantes entre os dois projetos. Enquanto o *NetDefense* é voltado para o ensino fundamental e médio, a proposta do *CyberWar* busca alcançar tanto usuários comuns quanto profissionais em ambientes corporativos. Além disso, o *NetDefense* foca na defesa de redes por meio de mecânicas estratégicas de *tower defense*, enquanto o jogo desenvolvido prioriza a conscientização sobre ameaças digitais enfatizando o impacto do fator humano na segurança digital. Dessa forma, esse trabalho expande o escopo da gamificação para além da defesa de redes, abordando a cibersegurança como um conjunto de boas práticas aplicáveis ao cotidiano digital de diferentes públicos.

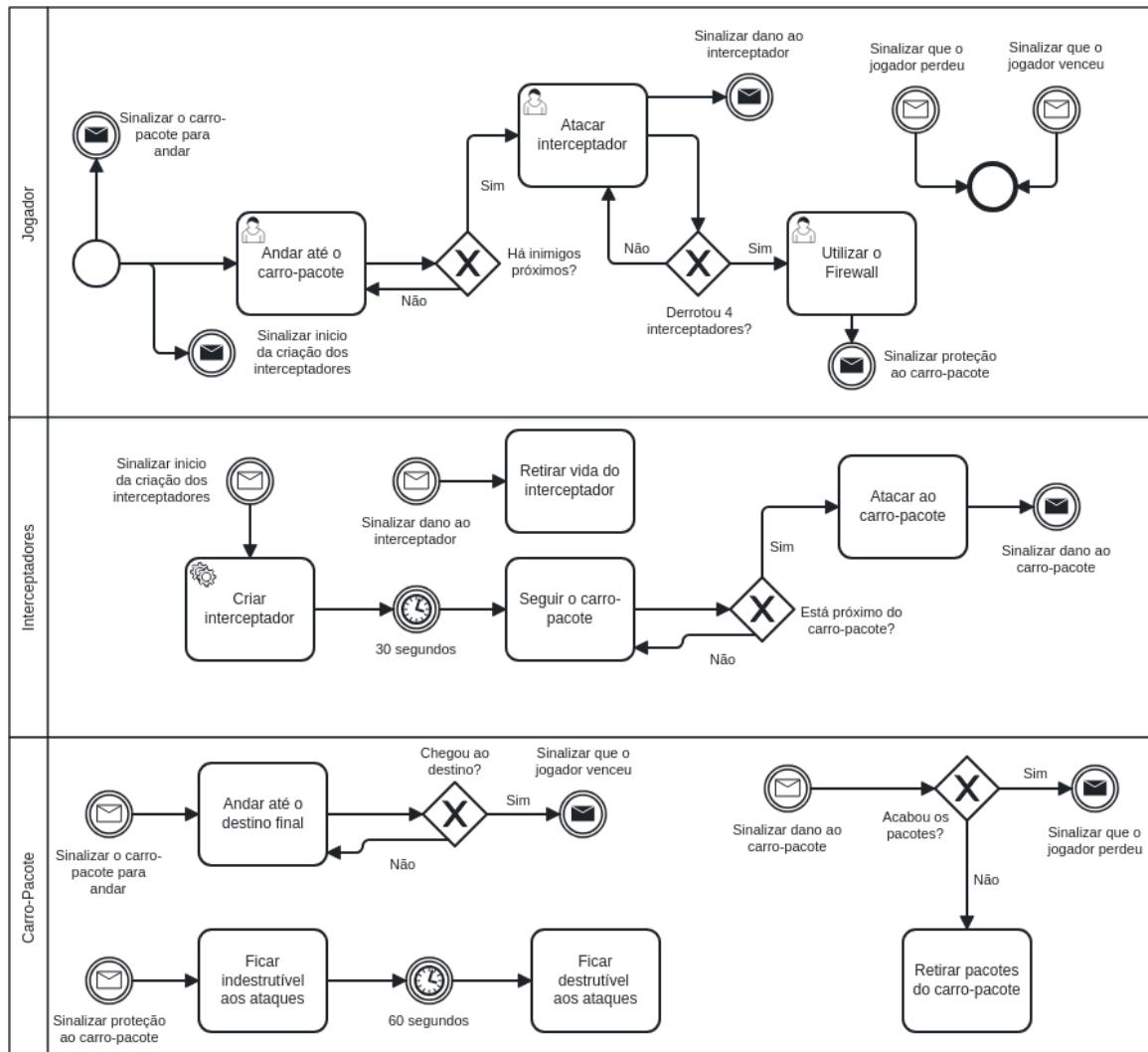
Por fim, o *CyberWar* representa uma contribuição relevante para o campo da educação em cibersegurança ao propor uma abordagem que integra o aprendizado técnico com a formação comportamental dos usuários. Enquanto muitos jogos educativos existentes focam em aspectos estruturais, como a proteção de redes e a filtragem de pacotes, o *CyberWar* inova ao abordar diretamente ameaças que exploram o fator humano, como o *phishing* e os ataques *man-in-the-middle*. Ao combinar uma narrativa com desafios práticos, o projeto oferece aos jogadores não apenas o conhecimento conceitual, mas também a oportunidade de aplicar, de forma lúdica, boas práticas de segurança no enfrentamento de situações realistas. Essa abordagem promove a conscientização ativa, incentivando mudanças no comportamento digital e reforçando a capacidade dos usuários de reconhecer e reagir a ataques cibernéticos no cotidiano. Além disso, ao direcionar seu conteúdo para públicos variados, incluindo usuários corporativos e educacionais, o *CyberWar* amplia o impacto da educação em segurança digital, tornando o aprendizado mais acessível, interativo e eficaz. Com isso, o projeto contribui para fortalecer a cultura de segurança da informação em diferentes contextos, atuando não apenas na transmissão de conhecimento, mas também na formação de atitudes preventivas essenciais para a redução de incidentes causados por falhas humanas.

4. CYBERWAR

O desenvolvimento do *CyberWar* teve origem na necessidade de ensinar cibersegurança de maneira acessível, prática e envolvente. Para alcançar esse objetivo, foi concebida uma narrativa interativa ambientada na fictícia Guarda Digital de Segurança, uma agência especializada na proteção de sistemas contra ameaças virtuais. Nessa história, o jogador assume o papel de um novato recém-integrado à equipe, que precisa, ao longo da jornada, aprender a identificar e combater diferentes tipos de ataques cibernéticos, impedindo que agentes mal-intencionados comprometam dados sensíveis. A narrativa é aprofundada com a presença de personagens não jogáveis (*Non-Playable Character - NPCs*) que têm a função de orientar o jogador quanto ao funcionamento dos minijogos e, ao mesmo tempo, apresentar os principais conceitos da

cibersegurança de forma lúdica e didática. Após a estruturação do enredo, deu-se início à seleção e criação dos elementos visuais e sonoros que integram o universo do jogo. Para isso, foram utilizados recursos disponíveis na *Unity Asset Store* e animações obtidas por meio da plataforma *Mixamo* (ADOBE, 2025), com o objetivo de compor uma estética coerente com os temas de tecnologia, programação e segurança digital. Foram escolhidos modelos de personagens, texturas, materiais, efeitos sonoros e animações que contribuíssem para a construção de uma identidade visual futurista. Os *NPCs* foram representados como robôs, simbolizando assistentes digitais, enquanto os cenários foram pensados para simular ambientes corporativos modernos, compostos por estações de trabalho e equipamentos tecnológicos. O personagem principal, por sua vez, recebeu uma caracterização com armamento de visual futurista, reforçando a ambientação voltada à defesa no ambiente digital. A seleção dos temas abordados nos minijogos foi fundamentada em dados atualizados sobre ameaças virtuais. O *phishing* está presente em 79% dos ataques de tomada de conta, conhecidos como *Account Takeover (ATO)*, sendo considerado a principal ameaça cibernética para 30% das pequenas empresas (SOCRADAR, 2024). Já os ataques do tipo *man-in-the-middle* são responsáveis por 19% dos ataques online bem-sucedidos e por 35% das explorações de redes *Wi-Fi* inseguras (SECURITY ESCAPE, 2024). Esses dados evidenciam a urgência de capacitar os usuários para reconhecer e mitigar essas ameaças, o que serviu como base para o desenvolvimento dos minijogos.

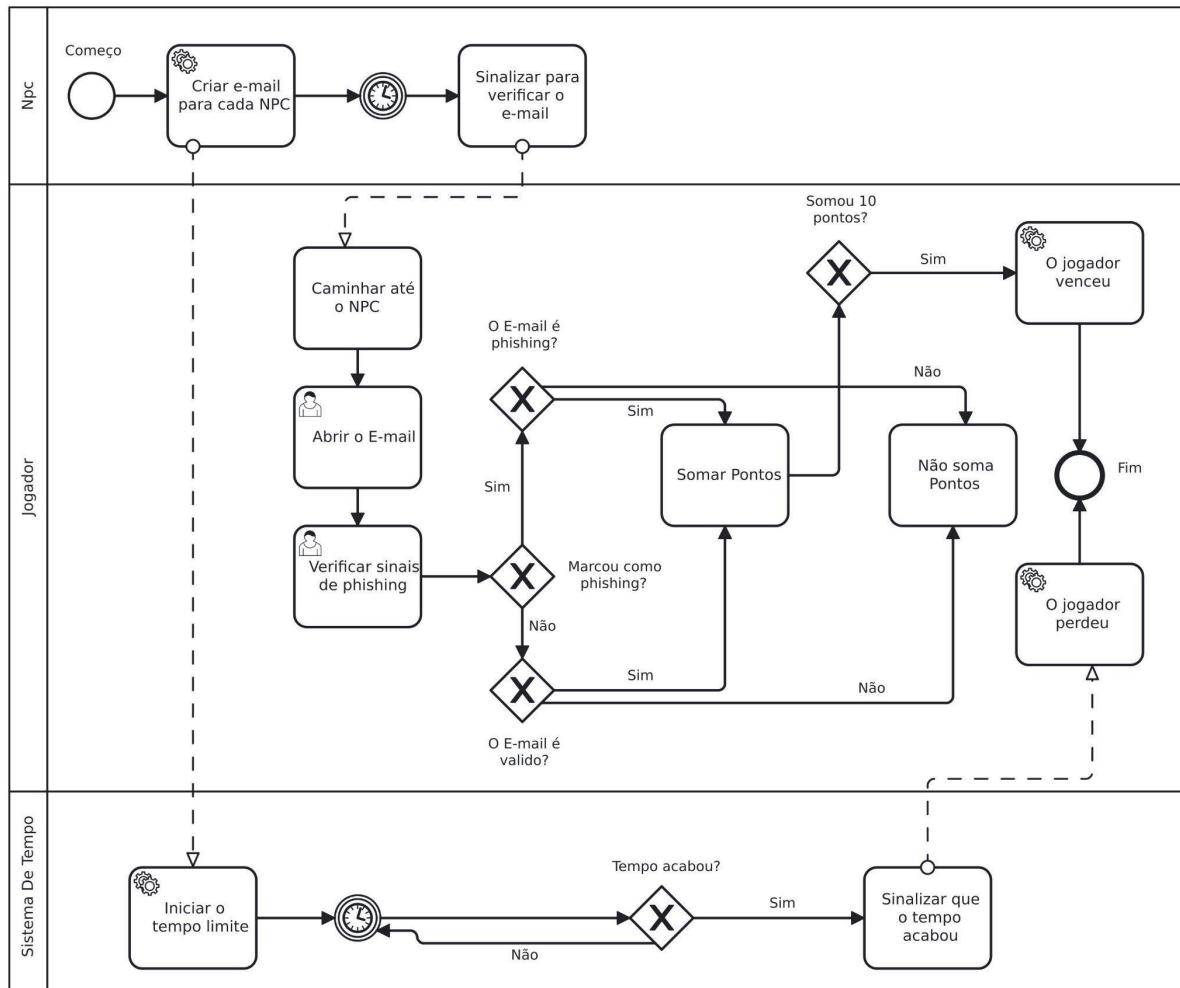
Dessa forma, foi desenvolvido um minijogo que simula um ataque *man-in-the-middle*, no qual o jogador é inserido em uma rede virtual que está trafegando dados, sendo que esse é encarregado de proteger o carro-pacote, uma representação metafórica do tráfego de dados sigilosos entre um emissor e um receptor. Durante o percurso, o veículo é alvo de interceptadores que tentam capturar os dados transmitidos. Para impedir que isso aconteça, o jogador conta com duas ferramentas principais: uma espada, que representa a criptografia e é usada para bloquear ataques diretos, e um *firewall* temporário, um recurso especial que torna o carro-pacote invulnerável por um curto intervalo de tempo. O desafio consiste em utilizar esses recursos de forma estratégica para impedir a interceptação dos dados, promovendo, assim, a compreensão prática de como mecanismos de proteção operam no contexto da segurança digital. Caso o inimigo consiga destruir o carro-pacote, a partida é encerrada com a derrota do jogador.

Figura 01 - Diagrama ilustrativo sobre o *minigame man-in-the-middle*

Fonte: elaborada pelos autores.

Por outro lado, foi idealizado para que no *minigame de phishing*, o jogador seja inserido no ambiente de uma empresa com diversos funcionários. Periodicamente, ele é chamado por *NPCs* para ajudá-los a analisar *emails* suspeitos. A missão consiste em identificar sinais típicos de fraude, avaliando quatro aspectos principais: a confiabilidade do remetente, a presença de erros gramaticais, a existência de *links* suspeitos e o uso de táticas de pressão psicológica. Ao identificar corretamente um *email* falso, o jogador ganha pontos e reforça seu conhecimento sobre como se proteger contra esse tipo de ataque no mundo real. No entanto, se não for ágil o suficiente, ele perde o jogo.

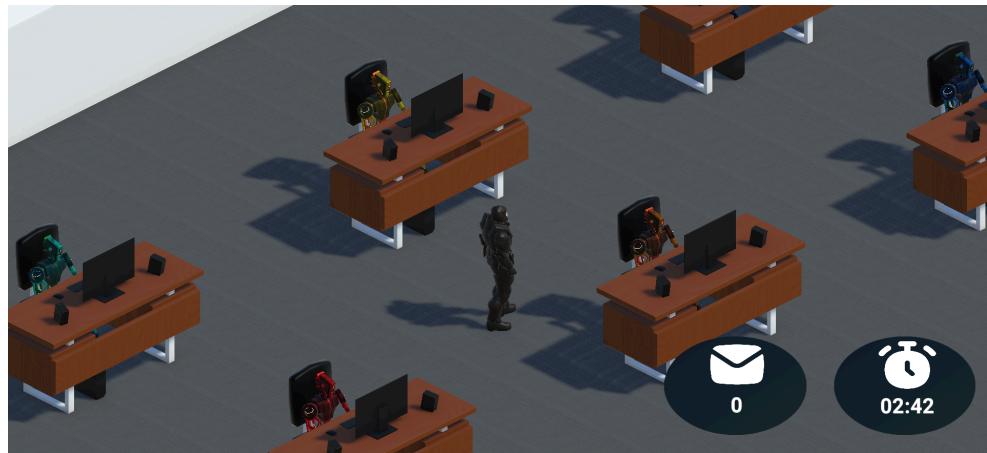
Figura 02 - Diagrama ilustrativo sobre o minigame phishing



Fonte: elaborada pelos autores

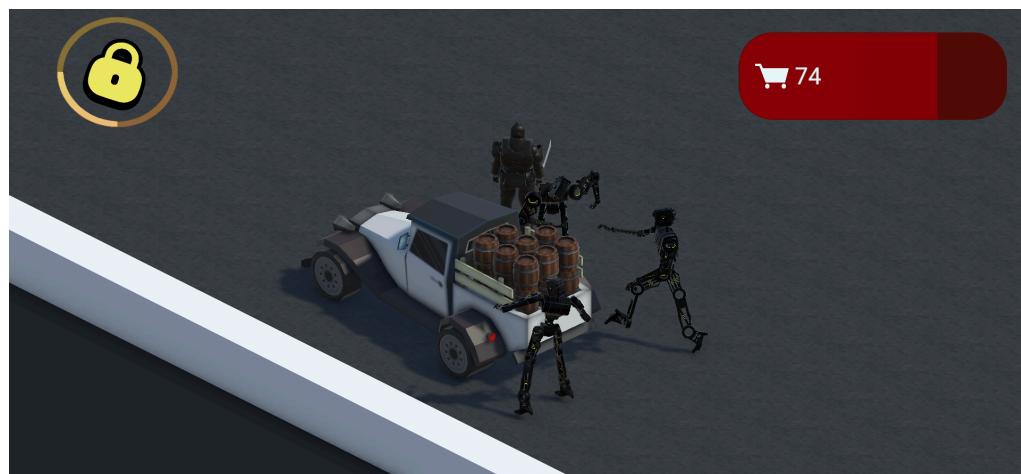
O jogo foi desenvolvido em um ambiente tridimensional (3D) com câmera isométrica, com o objetivo de proporcionar uma experiência imersiva alinhada aos princípios da DGBL. A ambientação foi construída com base em elementos da cibersegurança, integrando cenários temáticos, animações para *NPCs* e efeitos sonoros que reforçam o realismo e a imersão do jogador. O projeto passou por múltiplas sessões de testes, durante as quais as mecânicas foram ajustadas e balanceadas, garantindo uma jogabilidade acessível, justa e envolvente para diferentes perfis de usuários.

Figura 03 - Imagem ilustrativa do *minigame phishing*



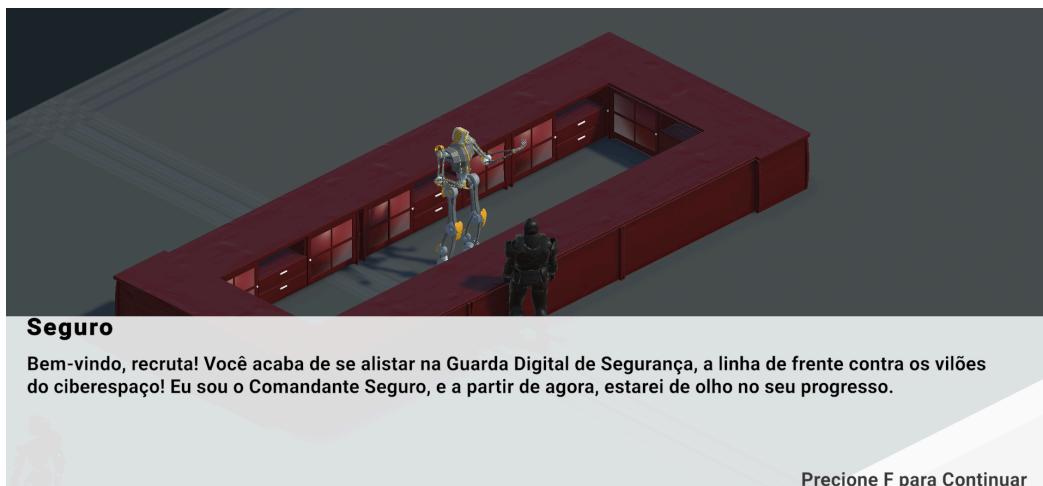
Fonte: elaborada pelos autores

Figura 04 - Imagem ilustrativa do *minigame man-in-the-middle*



Fonte: elaborada pelos autores

Figura 05 - Imagem ilustrativa do *Hub* com *NPC* que explica sobre conceitos de cibersegurança



Fonte: elaborada pelos autores

5. METODOLOGIA

Com o intuito de analisar o uso de jogos digitais no ensino de cibersegurança, esta pesquisa foi estruturada com uma abordagem metodológica capaz de abranger tanto percepções dos participantes quanto dados objetivos sobre a efetividade da proposta. A seguir, apresenta-se a classificação da pesquisa e as etapas que guiaram sua execução.

A presente pesquisa possui caráter exploratório e natureza aplicada, uma vez que o uso de jogos digitais como ferramenta de ensino em cibersegurança ainda representa um campo em desenvolvimento, com grande potencial para contribuir na conscientização sobre ameaças digitais. Para orientar o desenvolvimento do projeto, foi adotada a metodologia ágil *Scrum*. O uso do *Scrum* permitiu dividir o projeto em *sprints* bem definidas, com entregas incrementais e revisões constantes, facilitando a adaptação às necessidades emergentes e o aprimoramento contínuo do jogo com base no *feedback* dos usuários. Essa abordagem favoreceu a integração entre as etapas de desenvolvimento e pesquisa, garantindo maior alinhamento entre os objetivos educacionais e as funcionalidades do jogo. A pesquisa adotou também uma abordagem mista, combinando métodos qualitativos e quantitativos.

A realização desta pesquisa seguiu um conjunto de etapas planejadas, com o objetivo de garantir a consistência metodológica e a profundidade na análise dos resultados. O processo teve início com a identificação das principais questões sobre cibersegurança que o jogo busca abordar por meio de sua narrativa e mecânicas de *gameplay*. Com base nessas questões, foram elaborados dois questionários complementares. O primeiro teve como propósito mapear o conhecimento prévio dos participantes e suas experiências anteriores com métodos de ensino voltados à cibersegurança. Para isso, foram incluídas perguntas relacionadas a conceitos de ataques cibernéticos, engenharia social e práticas de segurança digital, além de questões voltadas ao perfil dos respondentes, como faixa etária, setor de trabalho, nível atual de conhecimento sobre o tema e participação em atividades educativas anteriores, como cursos ou palestras. O segundo questionário concentrou-se na avaliação da experiência com o jogo, investigando aspectos como os conhecimentos adquiridos, o grau de engajamento e a percepção geral sobre a temática após a interação com a proposta educativa. Nesse momento, as questões conceituais do primeiro questionário foram reaplicadas com a finalidade de mensurar o ganho de conhecimento, sendo acrescidas perguntas específicas sobre a experiência com o *game*, incluindo uma questão aberta destinada a colher sugestões e críticas construtivas para o aprimoramento da ferramenta. A amostra da pesquisa foi composta por 33 participantes, selecionados de forma intencional, com diferentes níveis de familiaridade com o tema e pertencentes a variadas faixas etárias. Os convites para participação foram realizados por meio de redes sociais, grupos acadêmicos e contatos

diretos, tendo como critério principal o interesse voluntário na atividade, independentemente da idade. Para viabilizar o acesso dos participantes à proposta desenvolvida, o jogo foi disponibilizado na plataforma *Unity Play*, em formato *Unity WebGL*, permitindo que fosse executado diretamente pelo navegador, sem a necessidade de instalação. Os *links* de acesso tanto ao jogo quanto aos questionários foram enviados individualmente aos participantes, assegurando a organização do processo e o controle das respostas. Após a coleta, os dados foram sistematizados em planilhas do *Excel*, o que possibilitou a geração de gráficos e contribuiu para uma análise minuciosa dos resultados obtidos. A investigação seguiu duas frentes complementares: a qualitativa e a quantitativa. A análise qualitativa concentrou-se nas respostas abertas do segundo questionário, destacando percepções, críticas e sugestões referentes à experiência com o jogo, fornecendo subsídios importantes para seu aprimoramento. Paralelamente, a análise quantitativa foi conduzida por meio da comparação entre os questionários aplicados antes e depois da interação com o game, o que permitiu mensurar o impacto da ferramenta tanto no aumento do conhecimento quanto no estímulo ao interesse pela cibersegurança. Por fim, a interpretação final dos resultados foi fundamentada na literatura especializada, confirmando a relevância da abordagem adotada e apontando caminhos promissores para melhorias e futuras aplicações do projeto.

Para tornar possível o desenvolvimento do *CyberWar*, foram adotadas tecnologias e recursos que contribuíram diretamente para a criação da experiência. O jogo foi desenvolvido na *Unity*, um motor gráfico amplamente utilizado na indústria de jogos, escolhido por sua flexibilidade, alto desempenho e ampla compatibilidade com diferentes plataformas, incluindo a exportação para *WebGL*, fator essencial para a disponibilização do jogo via navegador, sem a necessidade de instalação. A programação foi realizada em *C#* (MICROSOFT, 2025), linguagem nativa da *Unity*, que oferece robustez e vasto suporte da comunidade, facilitando a criação de funcionalidades como simulações interativas e mecânicas dinâmicas. Para enriquecer a ambientação e tornar a experiência mais realista, foram utilizados recursos visuais e sonoros provenientes da *Unity Asset Store*, que disponibiliza gratuitamente ou a preços acessíveis modelos *3D*, materiais, texturas e efeitos de áudio. Esses recursos são permitidos para uso em projetos não lucrativos, como é o caso deste jogo com fins educacionais. Além disso, o site *Mixamo* foi utilizado para importar animações realistas aplicadas aos personagens não jogáveis. O *Mixamo* também permite o uso gratuito de suas animações em jogos sem fins lucrativos, o que viabilizou a criação de interações mais naturais e dinâmicas entre os personagens e o jogador. A integração dessas ferramentas não apenas acelerou o processo de desenvolvimento, como também garantiu um alto nível de qualidade visual e interatividade, fundamentais para engajar o jogador e facilitar a assimilação de conceitos complexos de cibersegurança.

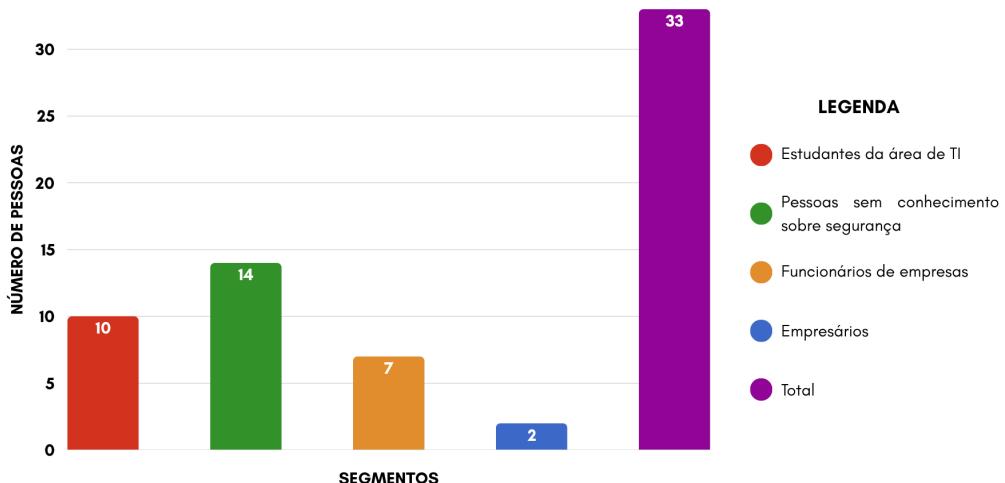
6. RESULTADOS

Nesta seção serão apresentados e analisados os dados coletados por meio da aplicação dos questionários de pré e pós-jogo, com o objetivo de avaliar o impacto do jogo educativo desenvolvido na aprendizagem dos participantes sobre cibersegurança.

6.1. Segmentos dos participantes

A presente pesquisa teve como a maior parte dos participantes formada por pessoas sem conhecimento sobre segurança da informação (14), seguida por estudantes da área de TI (10), funcionários de empresas (7) e, em menor número, empresários (2) (Figura 06). Essa distribuição indica que o *CyberWar* conseguiu alcançar um público diversificado, com predominância de indivíduos sem formação prévia na área, mas também incluindo profissionais e gestores. Esse perfil reforça a capacidade dos jogos digitais de adaptar a linguagem técnica a diferentes níveis de familiaridade, promovendo conscientização ampla e contribuindo para a formação de uma cultura de segurança mais acessível a todos os segmentos.

Figura 06 - Gráfico de segmentos dos participantes



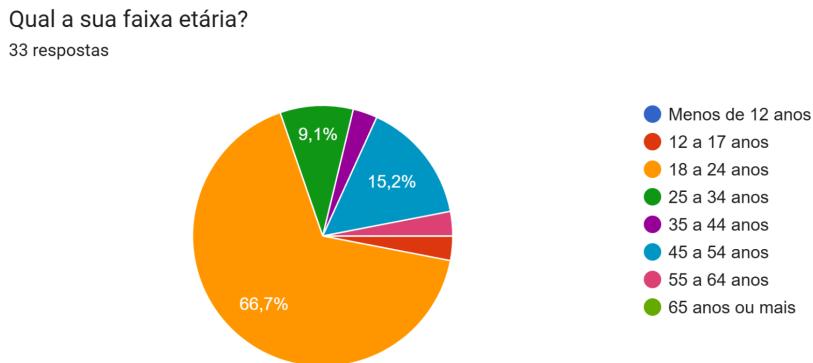
Fonte: elaborada pelos autores

6.2. Faixa etária dos participantes

O trabalho coletou a distribuição da faixa etária dos participantes da pesquisa (Figura 07). Observa-se que a maioria dos respondentes (66,7%) está na faixa de 18 a 24 anos, seguida por 15,2% entre 45 e 54 anos e 9,1% entre 25 e 42 anos. As demais faixas etárias tiveram participação irrelevante ou ausente. Embora a predominância seja de jovens adultos, a presença de indivíduos acima de 45 anos sugere que o interesse pelo tema e a usabilidade do jogo não se restringiram ao público mais jovem. Essa diversidade etária pode indicar que a proposta do *CyberWar* é acessível a diferentes perfis. Estudos anteriores apontam que jogos educativos podem ser adaptados a

públicos variados (CRIOLO-C et al., 2024; TOLEDO et al., 2022), o que reforça a possibilidade de aplicação inclusiva de jogos voltados à segurança digital.

Figura 07 - Gráfico de faixa etária dos participantes

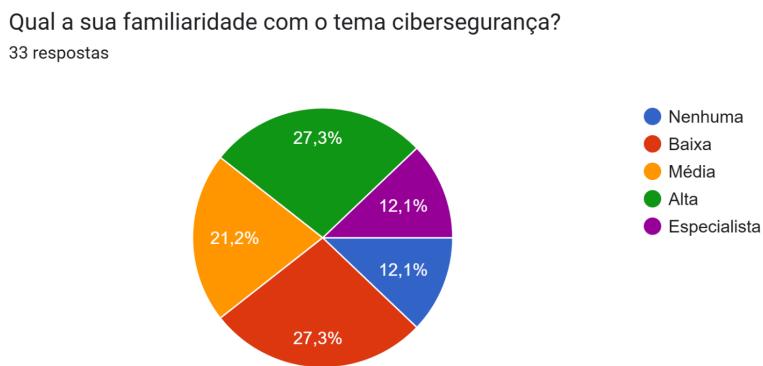


Fonte: elaborada pelos autores

6.3. Familiaridade com o tema cibersegurança (pré-jogo)

A pesquisa demonstrou a autopercepção dos participantes sobre seu conhecimento prévio em cibersegurança (Figura 08). A maioria relatou ter baixa (27,3%), média (21,2%) ou nenhuma (12,1%) familiaridade com o tema. Em contrapartida, 27,3% declararam ter alto conhecimento e 12,1% se consideram especialistas. Embora o número de participantes com familiaridade avançada seja significativo, ainda há uma parcela expressiva (mais de 60%) com conhecimentos limitados, o que evidencia a importância de estratégias educativas acessíveis. Jogos digitais com estrutura bem definida podem ser eficazes mesmo entre iniciantes, desde que contextualizam os conteúdos de forma prática (PIKI et al, 2023). O *CyberWar* foi estruturado nesse sentido, permitindo o acesso inicial a conteúdos técnicos sem exigir conhecimento prévio.

Figura 08 - Gráfico de familiaridade dos participantes com o tema cibersegurança

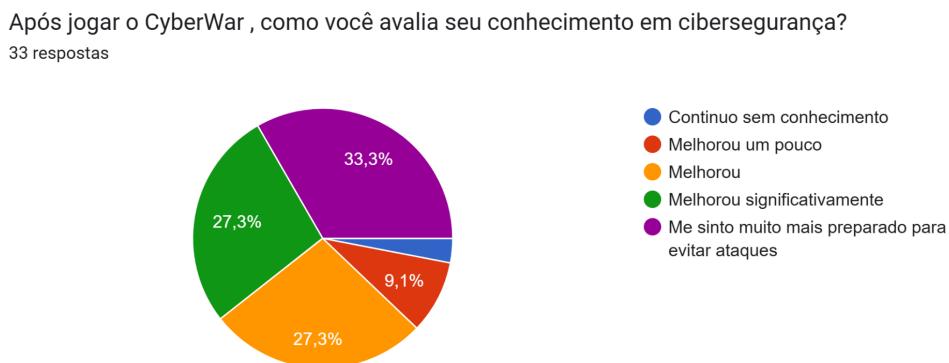


Fonte: elaborada pelos autores

6.4. Avaliação do conhecimento após o jogo

Os dados coletados mostraram que 33,3% dos participantes se sentiram muito mais preparados para evitar ataques após jogar o *CyberWar*, enquanto 27,3% relataram melhora significativa e outros 27,3% apontaram melhora moderada (Figura 09). Apenas 9,1% indicaram leve melhora e 3% afirmaram não ter adquirido conhecimento adicional. Esses resultados indicam um avanço na percepção pessoal de preparo para lidar com ameaças digitais, o que sugere que o uso de jogos digitais pode representar uma alternativa viável às abordagens tradicionais. A combinação de interatividade e desafio em jogos pode favorecer a aprendizagem com menor sobrecarga cognitiva (CRIOLLO-C et al, 2024), o que o *CyberWar* conseguiu alcançar, como mostrado no gráfico.

Figura 09 - Gráfico de avaliação do conhecimento dos participantes

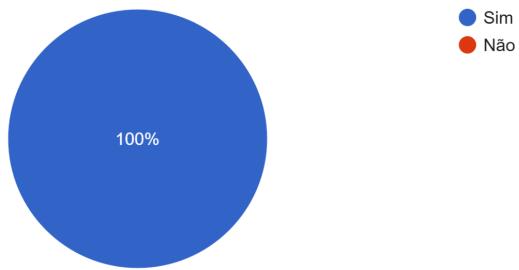


6.5. Entendimento sobre engenharia social

O jogo desenvolvido demonstrou que todos os participantes afirmaram compreender como ocorrem a engenharia social e ataques cibernéticos após jogarem (Figura 10). Esse dado sugere que a abordagem prática adotada no *CyberWar* contribuiu para facilitar a assimilação de um tema considerado abstrato. O uso de simulações pode ter sido determinante para esse resultado, o que está alinhado com conclusões de outros estudos sobre a eficácia de atividades lúdicas na compreensão de ameaças cibernéticas (PIKI et al., 2023).

Figura 10 - Gráfico de entendimento dos participantes sobre engenharia social

O jogo ajudou a entender melhor como os ataques de engenharia social ocorrem?
33 respostas



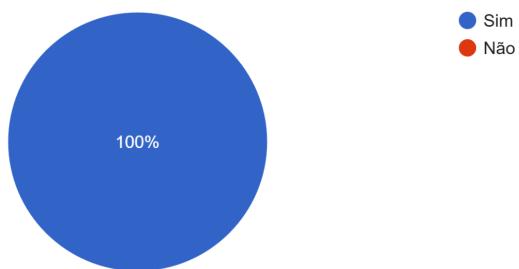
Fonte: elaborada pelos autores

6.6. Confiança para identificar tentativas de phishing

Os dados coletados demonstraram que 100% dos participantes declararam sentir-se confiantes para identificar tentativas de *phishing* após o jogo (Figura 11). A simulação de interações com *emails* suspeitos pode ter contribuído para esse resultado, permitindo o reconhecimento de padrões de ameaça em um ambiente controlado. Estudo similar identificou efeitos positivos na autoconfiança de usuários expostos a jogos com elementos de segurança digital (CRIOLLO-C et al., 2024).

Figura 11 - Gráfico de confiança dos participantes para identificar tentativas de phishing

Você se sente mais confiante para identificar tentativas de phishing e evitar ataques cibernéticos?
33 respostas



Fonte: elaborada pelos autores.

6.7. Interesse em aprender mais sobre cibersegurança

Após o uso do jogo, 90,9% dos participantes demonstraram interesse em continuar aprendendo sobre cibersegurança (Figura 12). Esse dado sugere que o *CyberWar* também desempenhou um papel motivacional, incentivando o engajamento futuro com o tema. Outros estudos também demonstraram que a estrutura narrativa e os desafios progressivos de jogos

educativos podem estimular o aprendizado autônomo (PIKI et al., 2023).

Figura 12 - Gráfico de interesse dos participantes em cibersegurança após o uso do jogo



Fonte: elaborada pelos autores.

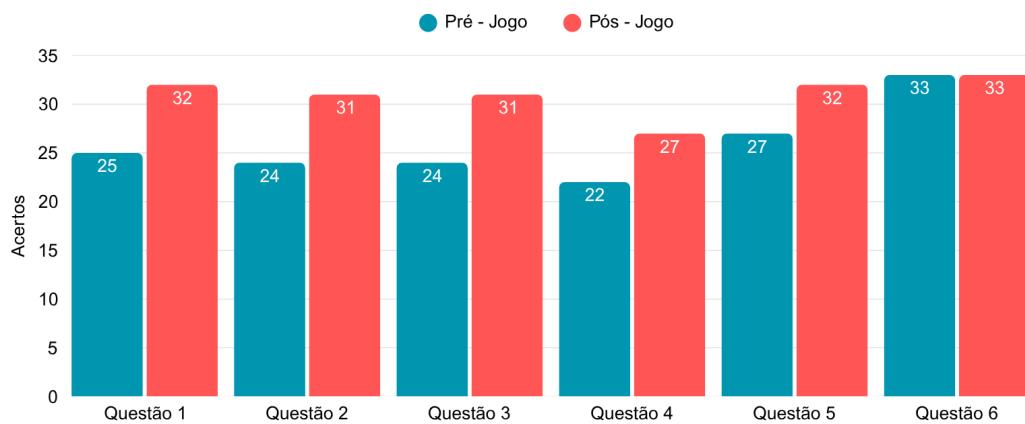
6.8. Desempenho geral (pré e pós-jogo)

A pesquisa realizada demonstrou um aumento no número de acertos nas questões do pós-teste em comparação ao pré-teste (Figura 13). Esse aumento demonstra que a experiência com o jogo contribuiu para a consolidação do conteúdo, indo além da percepção subjetiva dos participantes. Outros estudos também reportaram melhorias de desempenho com o uso de jogos gamificados no ensino de segurança cibernética (CRIOLLO-C et al., 2024).

Quadro 1 – Questões do formulário pré e pós-jogo

Nº da Questão	Questões
1	O que é phishing?
2	Qual destas situações representa um ataque de engenharia social?
3	Como funciona um ataque do tipo Man-in-the-Middle (MitM)?
4	O que fazer ao receber um e-mail suspeito pedindo que você clique em um link para redefinir sua senha?
5	Como evitar ataques de Man-in-the-Middle ao acessar redes Wi-Fi públicas?
6	Qual dessas práticas ajuda a minimizar riscos de engenharia social?

Fonte: elaborada pelos autores.

Figura 13 - Gráfico de desempenho geral dos participantes após o uso do jogo

Fonte: elaborada pelos autores.

6.9. Comparação das questões objetivas

A pesquisa apresentou percentuais de acerto em seis questões antes e depois da aplicação do jogo (Quadro 1). Em todas elas houve melhora, com destaque para as questões 1, 2 e 3, que apresentaram aumento de 21,2%. A média de acertos subiu de 78,28% para 93,93%, representando um ganho de 15,65%. A comparação entre os percentuais de acerto antes e depois do jogo confirma um ganho de conhecimento relevante em todos os tópicos avaliados, com destaque para os conteúdos mais vulneráveis à exploração por engenharia social e *phishing*. O aumento médio de 15,65% demonstra que mesmo usuários com pouca familiaridade inicial conseguiram absorver os conteúdos de forma significativa. Estudos similares também observaram resultados semelhantes ao aplicar jogos com foco em ameaças específicas, como o *NetDefense* (TOLEDO et al, 2022).

Quadro 2 – Percentual de acertos dos participantes por questão no formulário pré e pós-jogo

Nº da Questão	% Acertos Pré-Jogo	% Acertos Pós-Jogo	Variação
1	75,8%	97,0%	+21,2%
2	72,7%	93,9%	+21,2%
3	72,7%	93,9%	+21,2%
4	66,7%	72,7%	+15,4%
5	81,8%	97,0%	+15,2%
6	100%	100%	0%
Média	78,28%	93,93%	+15,65%

Fonte: elaborada pelos autores.

6.10. Discussão dos resultados

Os resultados alcançados com o jogo *CyberWar* demonstraram avanços significativos em relação às experiências pedagógicas anteriores com jogos digitais voltados ao ensino de cibersegurança, representadas por *CyberLearn2D* (PIKI et al., 2023), *CiberSecApp* (CRIOLLO-C et al., 2024) e *NetDefense* (TOLEDO et al., 2022). Enquanto esses projetos evidenciaram o potencial da gamificação para introduzir conceitos fundamentais e despertar o interesse dos usuários, o *CyberWar* ampliou essa visão ao demonstrar resultados tanto em termos cognitivos quanto comportamentais, consolidando uma nova perspectiva sobre o uso de jogos como recurso educacional em segurança digital. No caso do *CiberSecApp*, embora tenha havido uma melhora média de 14,47% no desempenho dos alunos entre o pré e o pós-teste, esse crescimento ficou restrito à assimilação de conceitos básicos e à avaliação da usabilidade da aplicação. O foco estava em tornar o conteúdo acessível e agradável, mas sem aprofundar a simulação de ameaças reais ou promover mudança comportamental duradoura. Já o *NetDefense*, voltado à compreensão técnica de redes, como pacotes e *firewalls*, teve seus resultados medidos pela autopercepção de professores do ensino básico, com 11 melhorias relatadas após a interação com o jogo. No entanto, os efeitos ficaram restritos à percepção de conhecimento, sem dados empíricos sobre retenção ou aplicação prática nos alunos. Por fim, o *CyberLearn2D* apresentou uma abordagem baseada em tarefas isoladas e *quizzes* sobre tópicos como *spam* e *phishing*, mas não forneceu dados quantitativos sobre os impactos da aprendizagem, limitando sua avaliação a reflexões pedagógicas sobre o *design* do jogo.

O *CyberWar*, por sua vez, amplia a visão ao articular narrativa envolvente, minijogos interativos e avaliação sistemática de resultados. Seus dados mostraram um avanço médio de 15,65% nos acertos gerais entre o pré e o pós-teste (Quadro 1), valor que se torna ainda mais expressivo ao observar que nas questões relacionadas a ataques sociais, como *phishing* e engenharia social, os acertos aumentaram até 21,2% (Quadro 1). No entanto, mais impactante foi o efeito comportamental e atitudinal: 100% dos participantes passaram a se considerar aptos a identificar ataques de *phishing* (Figura 11), e 100% entenderam claramente o conceito de engenharia social após o jogo (Figura 10), resultado que não foi alcançado por nenhum dos trabalhos anteriores. Isso demonstra que o *CyberWar* não apenas ensinou conteúdos, mas formou competências práticas e moveu autoconfiança digital. Além disso, o jogo despertou interesse contínuo em segurança da informação, com 90,9% dos participantes demonstrando disposição em continuar aprendendo sobre o tema (Figura 12). Essa capacidade de engajamento duradouro contrasta com os demais projetos, que focaram na introdução pontual de conteúdos. A diferença-chave está na imersão narrativa e no realismo das situações simuladas em *CyberWar*,

que possibilitaram aos jogadores experienciar ataques e responder a eles em tempo real. Isso ampliou o conceito de gamificação de um meio instrucional para uma ferramenta de vivência prática, onde o conhecimento é internalizado por meio da experiência e não apenas pelo conteúdo exposto.

Assim, ao apresentar resultados mensuráveis em termos de aprendizado, mudança de comportamento e engajamento autônomo dos participantes, o *CyberWar* não apenas confirmou o potencial dos jogos digitais no ensino de cibersegurança, como também expandiu o escopo da aprendizagem baseada em jogos digitais. O jogo demonstrou que é possível ensinar conteúdos complexos, promover atitudes conscientes e preparar usuários de forma mais eficaz para os desafios do mundo digital. Dessa forma, representa um avanço qualitativo em relação às abordagens tradicionais, estabelecendo uma nova referência para o uso de jogos digitais na promoção da cidadania cibernética.

7. CONCLUSÃO

Este trabalho desenvolveu e analisou o jogo digital educativo *CyberWar* como uma ferramenta para o ensino de cibersegurança, com foco em ataques do tipo *phishing* e *man-in-the-middle*, por meio de minijogos interativos ambientados em um cenário 3D isométrico com elementos narrativos e mecânicas práticas de aprendizagem. Os objetivos foram plenamente alcançados, pois o jogo permitiu aos participantes assimilar conceitos complexos de forma acessível, prática e motivadora, o que foi comprovado por meio da aplicação de questionários antes e depois da interação com o jogo. Os resultados foram compatíveis com as expectativas e indicaram uma evolução significativa no conhecimento dos participantes sobre segurança digital, sobretudo em relação à compreensão da engenharia social e à capacidade de identificar tentativas de *phishing*, com todos os usuários relatando maior confiança após a experiência. Apesar dos resultados positivos, o questionário evidenciou algumas limitações, como a necessidade de aprimoramento na jogabilidade. Em certos momentos, as mecânicas apresentaram-se rígidas e pouco responsivas, indicando a importância de refinamentos técnicos para tornar a experiência mais fluida e dinâmica. Outra limitação relevante foi a baixa participação de pessoas com mais de 30 anos, o que impediu uma avaliação mais ampla sobre a efetividade do jogo junto a faixas etárias mais altas, que também são vulneráveis a ataques cibernéticos. Ainda assim, a pesquisa demonstrou que jogos digitais educativos têm potencial para atuar como instrumento de transformação no ensino de temas técnicos e abstratos, promovendo aprendizado ativo, retenção de conteúdo e mudança de comportamento digital. Além disso, a pesquisa apresentou como os jogos digitais aumentam a disposição e atenção dos jogadores sobre temas que podem ser considerados abstratos e não reais. A principal contribuição deste trabalho foi demonstrar a

viabilidade e a eficácia do uso da gamificação como método de conscientização em cibersegurança, especialmente ao unir elementos visuais, narrativos e interativos em um produto funcional que pode ser utilizado tanto em contextos educacionais quanto corporativos. Para trabalhos futuros, sugere-se aumentar a quantidade de minijogos abordando outros tipos de ataques cibernéticos, aprimorar a interface do jogo com a criação de telas de pausa, melhorar os diálogos entre os *NPCs* para aumentar a imersão do jogador, polir as mecânicas de jogabilidade para garantir uma experiência mais fluida e envolvente e buscar jogadores que estejam em uma faixa etária superior aos 30 anos.

REFERÊNCIAS

- ADOBE. *Mixamo*. Disponível em: <https://www.mixamo.com/>. Acesso em: 20 maio 2025.
- AFONSO, Lisa; RODRIGUES, Rui; REIS, Eduardo; MILLER, Kylee; CASTRO, Joana; PARENTE, Nuno; TEIXEIRA, Carina; FRAGA, Ana; TORRES, Sandra; Fammeal. **A Gamified Mobile Application for Parents and Children to Help Healthcare Centers Treat Childhood Obesity**. IEEE Explore, v. 12, ed. 4, n. 4 dez. 2020. Disponível em: <https://ieeexplore.ieee.org.ez93.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=9165016>. Acesso em: 29 mar. 2024.
- CRİOLLO-C, Santiago; GUERRERO-ARIAS, Andrea; BUENAÑO-FERNÁNDEZ, Diego; LUJÁN-MORA, Sergio. **Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study**. IEEE Access, [S. l.], p. 12771 - 12784, 11 jan. 2024. DOI 10.1109/ACCESS.2024.3352589. Disponível em: <https://ieeexplore.ieee.org/document/10388296>. Acesso em: 7 mar. 2025.
- FEDERAÇÃO BRASILEIRA DE BANCOS. **Pesquisa Febraban de Tecnologia Bancária 2024: Volume 2**. Realizada pela Deloitte. Disponível em: <https://portal.febraban.org.br/noticia/4146/pt-br/>. Acesso em: 31 mar. 2025.
- G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal**. 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em: 31 mar. 2025.
- KUO, Chun-Hsin; CHEN, Meng-Jun; NABABAN, Robasa; SHE, Hsiao-Ching. **Space Adventure Game-Based Learning: How Games and Scaffolds Affect Eighth Graders' Physics Learning and Game Immersion**. IEEE Transactions on Learning Technologies, IEEE Xplore, v. 17, p. 229-240, 23 jun. 2023. DOI 10.1109/TLT.2023.3288879. Disponível em: <https://ieeexplore.ieee.org.ez93.periodicos.capes.gov.br/document/10160196>. Acesso em: 5 mar. 2025.
- LÓPEZ-FERNÁNDEZ, Daniel et al. **Comparing Traditional Teaching and Game-Based Learning Using Teacher-Authored Games on Computer Science Education**. IEEE Transactions on Education, IEEE Xplore, v. 64, p. 367 - 373, 12 mar. 2021. DOI 10.1109/TE.2021.3057849. Disponível em: <https://ieeexplore.ieee.org/document/9377551>. Acesso em: 31 mar. 2025.
- MICROSOFT. *Documentação do C#*. Disponível em: <https://learn.microsoft.com/pt-br/dotnet/csharp/>. Acesso em: 20 maio 2025
- NASUTION, Mutiara; LUBIS, Muhamar; SAEDUDIN, RD. Rohmat; WIDJAJARTO, Adityas. **Defense in Depth Strategy from Phising Attacks in Using Instagram**. 2024 International Conference on Data Science and Its Applications (ICoDSA), IEEE Xplore, p. 1-6, 5 set. 2024. DOI 10.1109/ICoDSA62899.2024.10651679. Disponível em: <https://ieeexplore.ieee.org.ez93.periodicos.capes.gov.br/document/10651679>. Acesso em: 6 mar. 2025.

PIKI, Andriani; STAVROU, Eliana; PROCOPIOU, Andria; DEMOSTHENOUS, Anthimos. **Fostering Cybersecurity Awareness and Skills Development Through Digital Game-Based Learning.** 2023 10th International Conference on Behavioural and Social Computing (BESC), IEEE Xplore, p. 1-6, 17 jan. 2024. DOI 10.1109/BESC59560.2023.10386988. Disponível em: <https://ieeexplore-ieee-org.ez93.periodicos.capes.gov.br/document/10386988>. Acesso em: 5 mar. 2025.

SAED, Muhanna; ALJUHANI, Ahamed. **Detection of Man in The Middle Attack using Machine learning.** 2022 2nd International Conference on Computing and Information Technology (ICCIT), IEEE Xplore, p. 1-6, 17 fev. 2022. DOI 10.1109/ICCIT52419.2022.9711555. Disponível em: <https://ieeexplore-ieee-org.ez93.periodicos.capes.gov.br/document/9711555>. Acesso em: 6 mar. 2025.

SANGWAN, Aarti. **Human Factors in Cybersecurity Awareness.** 2023 International Conference on Communication, Computing and Digital Systems (C-CODE), IEEE Xplore, p. 1-7, 12 jul. 2024. DOI 10.1109/ISCS61804.2024.10581139. Disponível em: <https://ieeexplore-ieee-org.ez93.periodicos.capes.gov.br/document/10581139>. Acesso em: 5 mar. 2025.

SANTIAGO, Jesús; MACOTELA, Coraly; CASTILLO, Hector; MAYTA, Geraldine. **Use of 2D/3D Video Games in Digital Platforms for Basic Education: A Technological and Systematic Review.** IEEE Explore, Colombian Caribbean Conference (C3), 21 fev. 2024. DOI 10.1109/C358072.2023.10436294. Disponível em: <https://ieeexplore-ieee-org.ez93.periodicos.capes.gov.br/document/10436294>. Acesso em: 20 jun. 2024.

SCHWABER, Ken; SUTHERLAND, Jeff. *Guia do Scrum: a definição do Scrum.* 2020. Disponível em: <https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-PortugueseBR-3.0.pdf>. Acesso em: 20 maio 2025.

SECURITY ESCAPE. **Man-in-the-Middle Attack Statistics.** 2024. Disponível em: <https://securityescape.com/man-in-the-middle-attack-statistics>. Acesso em: 2 abr. 2025.

SENHASEGURA. **Estatísticas de cibersegurança: tendências e previsões para 2024 e além.** 2024. Disponível em: <https://senhasegura.com/pt-br/post/estatisticas-de-ciberseguranca>. Acesso em: 31 mar. 2025.

SOCRADAR. **Top 50 Cybersecurity Statistics in 2024: Essential Insights on Ransomware, Phishing, Industry Trends and More.** 2024. Disponível em: <https://socradar.io/top-50-cybersecurity-statistics-in-2024-essential-insights-on-ransomware-phishing-industry-trends-and-more>. Acesso em: 2 abr. 2025.

SREEHARI, S; GOKULAPRIYA, R. **Comparing Developmental Approaches for GameBased Learning in Cyber-Security Campaigns.** IEEE International Conference on Contemporary Computing and Communications, IEEE Xplore, p. 1-7, 22 abr. 2022. DOI 10.1109/InC457730.2023.10263260. Disponível em: <https://ieeexplore.ieee.org/document/10263260/metrics#metrics>. Acesso em: 31 mar. 2025.

TOLEDO, William; LOUIS, Sushil J; SENGUPTA, Shamik. **NetDefense: A Tower Defense Cybersecurity Game for Middle and High School Students.** 2022 IEEE Frontiers in Education Conference (FIE), [S. l.], p. 1-6, 29 nov. 2022. DOI 10.1109/FIE56618.2022.9962410. Disponível em: <https://ieeexplore.ieee.org/document/9962410/authors>. Acesso em: 7 mar. 2025.

UNITY TECHNOLOGIES. *Unity Documentation*. Disponível em: <https://docs.unity.com/>. Acesso em: 20 maio 2025.

ZHAO,Dan;MUNTEAN,Cristina;CHRIS,Adriana. **GAME-BASED Learning: Enhancing Student Experience, Knowledge Gain, and Usability in Higher Education Programming Courses.** IEEE Explore, v. 65, ed. 4, n. 4 nov. 2022. Disponível em: <https://ieeexplore-ieee-org.ez93.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=9675819&tag=1>. Acesso em: 28 mar. 2024.