Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional para o Ensino de Cibersegurança no Ensino Fundamental I e II

Jeanluca Martins de Abreu

Universidade Federal de Uberlândia
Faculdade de Computação
Programa de Pós-Graduação em Ciência da Computação

Uberlândia
2026

Jeanluca Martins de Abreu

Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional para o Ensino de Cibersegurança no Ensino Fundamental I e II

Dissertação de mestrado apresentada ao Programa de Pós-graduação da Faculdade de Computação da Universidade Federal de Uberlândia como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Sistemas de Computação

Orientador: Diego Nunes Molinos
Coorientador: Rafael Dias Araújo

Uberlândia
2026

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

A162 Abreu, Jeanluca Martins de, 1998-
2026 Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional para o Ensino de Cibersegurança no Ensino Fundamental I e II [recurso eletrônico] / Jeanluca Martins de Abreu. - 2026.

Orientador: Diego Nunes Molinos.
Coorientador: Rafael Dias Araújo.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Ciência da Computação.
Modo de acesso: Internet.
DOI http://doi.org/10.14393/ufu.di.2026.513
Inclui bibliografia.
Inclui ilustrações.

1. Computação. I. Molinos, Diego Nunes,1986-, (Orient.). II. Araújo, Rafael Dias,1986-, (Coorient.). III. Universidade Federal de Uberlândia. Pós-graduação em Ciência da Computação. IV. Título.

CDU: 681.3

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Computação
Av. João Naves de Ávila, 2121, Bloco 1A, Sala 243 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4470 - www.ppgco.facom.ufu.br - cpgfacom@ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Ciência da Computação				
Defesa de:	Dissertação, 17/2026, PPGCO				
Data:	08 de Julho de 2026	Hora de início:	15:00	Hora de encerramento:	17:15
Matrícula do Discente:	12412CCP011				
Nome do Discente:	Jeanluca Martins de Abreu				
Título do Trabalho:	Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional para o Ensino de Cibersegurança no Ensino Fundamental I e II				
Área de concentração:	Ciência da Computação				
Linha de pesquisa:	Sistemas de Computação				
Projeto de Pesquisa de vinculação:	----------				

Reuniu-se por videoconferência, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Ciência da Computação, assim composta: Professores Doutores: Rafael Dias Araújo - FACOM/UFU (Coorientador), Renan Gonçalves Cattelan - FACOM/UFU, Marcela Sávia Picanço Pessoa - EST/UEA e Diego Nunes Molinos - FACOM/UFU, orientador do(a) candidato(a).

Os examinadores participaram desde as seguintes localidades: Marcela Sávia Picanço Pessoa - Manaus/AM e os outros membros da banca da cidade de Uberlândia/MG. O aluno Jeanluca Martins de Abreu participou de Matipó/MG.

Iniciando os trabalhos o(a) presidente da mesa, Prof. Dr. Diego Nunes Molinos, apresentou a Comissão Examinadora e o(a) candidato(a), agradeceu a presença do público, e concedeu ao(à) Discente a palavra para a exposição do seu trabalho.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato(a):

Aprovado

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Diego Nunes Molinos**, **Professor(a) do Magistério Superior**, em 13/07/2026, às 08:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Renan Gonçalves Cattelan**, **Professor(a) do Magistério Superior**, em 13/07/2026, às 10:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rafael Dias Araújo**, **Professor(a) do Magistério Superior**, em 13/07/2026, às 12:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcela Sávia Picanço Pessoa Bastos**, **Usuário Externo**, em 14/07/2026, às 10:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7455817** e o código CRC **81E5483B**.

Referência: Processo nº 23117.044163/2026-30 SEI nº 7455817

Dedico este trabalho, com todo o amor e carinho, aos meus pais, José e Maria, pelo apoio incondicional, pelo incentivo constante e por sempre acreditarem nos meus sonhos. Tudo o que conquistei até hoje devo ao amor e ao suporte de vocês. Obrigado por nunca desistirem de mim.

Aos meus amigos, pela cumplicidade, pelo companheirismo e pelas pausas necessárias que tornaram esta jornada mais leve e acolhedora. O apoio de vocês fez toda a diferença ao longo desta caminhada.

Ao meu orientador e ao meu coorientador, pela primorosa condução, pela paciência e pela generosidade no compartilhamento de conhecimentos essenciais para a realização deste trabalho. Suas orientações foram fundamentais para que este projeto se tornasse realidade.

Aos demais colaboradores e amigos que tornaram possível a conclusão deste ciclo tão importante, os meus mais sinceros agradecimentos!

Agradecimentos

Este trabalho é o resultado de uma longa jornada que não teria sido possível sem o apoio de pessoas essenciais. Aos que colaboraram, direta ou indiretamente, para que este momento se concretizasse, o meu muito obrigado.

Aos meus pais, José e Maria, pelo apoio incondicional, pelo incentivo constante e por sempre acreditarem nos meus objetivos e sonhos.

Aos meus amigos, pelo companheirismo, pelo apoio e pelos momentos de descontração que tornaram essa jornada mais leve.

Ao meu orientador e ao meu coorientador, pela dedicação, paciência, orientação e pelos valiosos ensinamentos compartilhados ao longo de todo o desenvolvimento deste projeto.

A todos os professores que fizeram parte da minha formação acadêmica e profissional, contribuindo de maneira fundamental para minha trajetória.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelo apoio e incentivo à pesquisa que possibilitaram a realização deste trabalho.

Por fim, agradeço a todos aqueles que contribuíram, de alguma forma, para a conclusão desta importante etapa da minha vida. Muito obrigado!

"A imaginação é a faculdade descobridora, por excelência. É ela que penetra nos mundos invisíveis ao nosso redor, os mundos da Ciência."

(Ada Lovelace)

Resumo

O aumento do acesso precoce de crianças e adolescentes às redes sociais, aliado ao crescimento dos casos de ataques cibernéticos, evidencia uma preocupação significativa quanto à segurança digital desse público. Diante desse cenário de crescente exposição a riscos no ambiente virtual, torna-se necessário desenvolver estratégias educacionais capazes de promover a conscientização e a adoção de práticas seguras no uso das tecnologias digitais. Essa necessidade é reconhecida pela Base Nacional Comum Curricular (BNCC), que incentiva o desenvolvimento de competências relacionadas ao uso crítico, ético e responsável das tecnologias digitais. Nesse contexto, esta dissertação apresenta o processo de desenvolvimento e a avaliação do Encrypta, um jogo digital educacional projetado para promover a conscientização sobre práticas seguras no ambiente digital entre estudantes da educação básica, principalmente do Ensino Fundamental I e II. O jogo aborda tópicos da área de cibersegurança, tais como a criação de senhas seguras, a identificação de arquivos, sites e e-mails maliciosos, e a importância da realização de *backups*. Esta pesquisa possui caráter exploratório por investigar uma temática ainda em consolidação no contexto educacional e buscar compreender como elementos relacionados aos jogos digitais contribuem para a aprendizagem em cibersegurança. Para isso, foram empregados instrumentos para mensurar a eficácia da solução proposta. O estudo foi realizado com estudantes do Ensino Fundamental I e II do Colégio de Aplicação da Universidade Federal de Uberlândia (CAp/UFU), por meio da aplicação do jogo educacional e da coleta de dados quantitativos e qualitativos, com o objetivo de avaliar a aprendizagem, a usabilidade e a percepção dos participantes em relação à ferramenta. Os principais resultados indicam um aumento no nível de conhecimento dos estudantes, além de avaliações positivas quanto à usabilidade e à experiência do jogador durante o uso da aplicação, evidenciando o potencial do jogo como ferramenta de apoio ao ensino de cibersegurança.

Palavras-chave: Jogos Digitais Educacionais. Cibersegurança. Aprendizagem Baseada em Jogos. Tecnologias Educacionais.

Abstract

The significant increase in the number of cyberattacks in the country, combined with the growing use of digital devices by children and adolescents, highlights a major concern regarding the safety of these individuals in the online environment. Given this situation, it is necessary to develop educational strategies that can promote awareness and the adoption of safe practices in the use of digital technologies. This need is also recognized by the National Common Curriculum Base (BNCC), which encourages the development of skills related to the critical, ethical, and responsible use of digital technologies. In this context, this dissertation proposes Encrypta, an educational digital game developed to support cybersecurity education for elementary school students. The application addresses fundamental topics in the field, including the creation of secure passwords, the identification of malicious files, websites, and emails, as well as the importance of performing backups. Methodologically, this research is exploratory in nature, as it investigates a topic that is still emerging within the educational context and seeks to understand how elements related to digital games contribute to cybersecurity learning. The effectiveness of the proposed solution was assessed through the application of evaluation instruments. The study was conducted with elementary school students at the Application School of the Federal University of Uberlândia (CAp/UFU) through the use of the educational game developed for this purpose and the collection of quantitative and qualitative data, with the aim of evaluating the participants' learning, the tool's usability, and their perceptions of it. The main results indicate an increase in students' knowledge levels, as well as positive evaluations regarding usability and user experience while using the application, highlighting the game's potential as a tool to support cybersecurity education.

Keywords: Educational Digital Games. Cybersecurity. Game-Based Learning. Educational Technologies.

Lista de ilustrações

Lista de tabelas

Lista de siglas

APK *Android Package Kit*

BNCC Base Nacional Comum Curricular

CAAE Certificado de Apresentação para Apreciação Ética

CAp/UFU Colégio de Aplicação da Universidade Federal de Uberlândia

CEP Comitê de Ética em Pesquisa com Seres Humanos

DDoS *Distributed Denial of Service*

DSR *Design Science Research*

HTTP *Hypertext Transfer Protocol*

IBGE Instituto Brasileiro de Geografia e Estatística

PDF *Portable Document Format*

PoC *Proof of Concept*

RQs *Research Questions*

RPG *Role-Playing Game*

SSL *Secure Sockets Layer*

TA Termo de Assentimento

TCLE Termo de Consentimento Livre e Esclarecido

TEA Transtorno do Espectro Autista

TDAH Transtorno do Déficit de Atenção e Hiperatividade

UFU Universidade Federal de Uberlândia

URLs *Uniform Resource Locator*

Sumário

Capítulo 1

Introdução

De acordo com dados divulgados pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2025, o Brasil possuía uma população de 213 milhões de habitantes (IBGE, 2025). Neste mesmo ano, a pesquisa de Meirelles (2025) apontou a existência de aproximadamente 480 milhões de dispositivos conectados à internet no país, abrangendo computadores, *notebooks*, *tablets* e *smartphones*, totalizando uma média de 2,2 aparelhos por habitante. O estudo mostrou que havia, em média, cerca de um *smartphone* por habitante em todo o mundo em 2025. Ainda de acordo com Meirelles (2025), entre as pessoas da faixa etária de 16 a 64 anos, os jovens de 16 a 24 anos estão entre os grupos que mais consomem internet diariamente.

No Brasil, o tempo médio de uso da internet em dispositivos móveis atinge cerca de 9 horas e 12 minutos por dia, aumentando para quase 10 horas diárias entre os jovens de 16 a 24 anos, o que posiciona o país como o segundo maior consumidor mundial. Conforme DataReportal (2026), em 2025, o Brasil contava com aproximadamente 185 milhões de usuários de internet, dos quais cerca de 150 milhões utilizavam ativamente mídias sociais, o que corresponde a 70,4% da população.

De acordo com Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) (2024), crianças e adolescentes de 9 a 17 anos, 76% afirmaram utilizar redes sociais, e 71% relataram acessar o WhatsApp[1] várias vezes ao dia ou diariamente, enquanto 66% apresentaram a mesma frequência de uso para o YouTube, 60% para o Instagram e 50% para o TikTok. Esses dados evidenciam o elevado nível de engajamento de crianças e adolescentes com plataformas digitais, como Instagram[2], TikTok[3], YouTube[4] e Facebook[5].

Considerando os dados apresentados, o uso frequente de redes sociais e outras plataformas digitais por crianças e adolescentes amplia sua exposição ao ambiente virtual e,

[1] https://www.whatsapp.com/
[2] https://www.instagram.com/
[3] https://www.tiktok.com/
[4] https://www.youtube.com/
[5] https://www.facebook.com/

consequentemente, aos riscos associados a esse contexto, como golpes, fraudes e ataques cibernéticos. De acordo com Trend Micro (2025), foi revelado que cerca de 168 milhões de tentativas de ataque virtuais por meio de *malwares*[6] ocorreram em 2024, além de mais de 240 mil casos de ataques de *ransomware*[7] identificados, o que posiciona o Brasil entre os países que registraram o maior volume de ameaças cibernéticas no mundo.

Em 2025, a empresa de cibersegurança Check Point (2026) apontou que o Brasil esteve entre os mais visados por *infostealers*[8], um tipo de *malware* que atua silenciosamente para roubar dados de usuários. Ainda de acordo com a pesquisa, o país lidera o ranking mundial, ao lado da Índia, sendo responsável por cerca de 7% dos ataques globais. Além disso, o país continua entre os principais alvos de ataques de *ransomware*.

1.1 Justificativa

Negligenciar a conscientização da população brasileira, em especial de crianças e adolescentes, sobre os riscos presentes no ambiente virtual pode expô-los a sérias ameaças, uma vez que pessoas com pouco ou nenhum conhecimento acerca dos crimes cibernéticos tornam-se alvos fáceis para os criminosos digitais (SILVA et al., 2025). Diante disso, a inserção da educação digital nas instituições de ensino brasileiras configura-se como uma estratégia essencial para promover a conscientização dos estudantes, oferecendo recursos que os capacitem a reconhecer e enfrentar situações de risco na internet.

Entretanto, abordar conceitos relacionados à segurança digital no contexto da educação básica representa um desafio, uma vez que temas como privacidade, proteção de dados e ameaças cibernéticas podem ser percebidos como abstratos ou pouco atrativos para os estudantes. Nesse sentido, torna-se necessário adotar abordagens pedagógicas capazes de despertar o interesse dos alunos e de favorecer sua participação ativa no processo de aprendizagem.

Neste contexto, os jogos digitais emergem como uma alternativa promissora no âmbito educacional, atuando como ferramentas capazes de complementar práticas tradicionais de ensino (CÔRTES; PAIXÃO, 2023). Ao combinar elementos de desafio, interação e entretenimento, esses recursos podem aumentar a motivação e o engajamento dos estudantes, favorecendo sua participação ativa no processo de aprendizagem. Em virtude dessas características, diversos trabalhos na área de Informática na Educação reconhecem os jogos digitais como instrumentos pedagógicos eficazes para apoiar a aprendizagem significativa e o desenvolvimento de competências em diferentes domínios do conhecimento

[6] *Malwares* são programas desenvolvidos para comprometer os dispositivos das vítimas, podendo causar danos, roubar informações ou permitir acesso não autorizado.

[7] *Ransomware* é uma categoria de *malware* desenvolvida para impedir o acesso a sistemas ou arquivos, normalmente por meio de criptografia, com o objetivo de extorquir a vítima mediante a cobrança de um resgate.

[8] *Infostealers* são programas maliciosos desenvolvidos para coletar informações sensíveis, como credenciais de acesso, dados bancários e informações pessoais armazenadas nos dispositivos das vítimas.

(PIETRUCHINSKI et al., 2011; SILVA; MEDEIROS; ARANHA, 2014; BATTISTELLA; WANGENHEIM, 2016).

Sob a óptica pedagógica, construtivista e socioconstrutivista, de acordo com Piaget (1976) e Vygotsky (1991), o jogo constitui uma forma privilegiada de construção do conhecimento, especialmente na infância e na adolescência, ao mediar o desenvolvimento cognitivo e social por meio da interação com o ambiente e com outros indivíduos. Complementando essa visão, autores contemporâneos, como Papert (1980), argumentam que ambientes lúdicos favorecem a aprendizagem ativa e a resolução de problemas. Assim, ao integrar elementos de jogos digitais ao processo educacional, é possível criar experiências que estimulem o raciocínio, a autonomia e a retenção de conteúdos relevantes. Essa abordagem é especialmente promissora em temas como a cibersegurança, pois permite o desenvolvimento de competências essenciais para identificar e reagir a situações práticas do cotidiano digital.

1.2 Motivação

A Base Nacional Comum Curricular (BNCC) BRASIL - Ministério da Educação (2022), passou a enfatizar o desenvolvimento de competências relacionadas ao uso crítico, seguro e responsável das tecnologias digitais. Entre essas competências destacam-se a verificação da confiabilidade das informações, a compreensão de mecanismos de armazenamento de dados, a identificação de fontes seguras e a introdução aos fundamentos da cibersegurança. Ao incorporar esses conteúdos ao currículo da educação básica, essas diretrizes ampliam a necessidade de recursos pedagógicos capazes de apoiar os professores na abordagem desses temas de forma acessível e contextualizada.

Além dos desafios relacionados à implementação dessas competências no contexto escolar, observa-se que os recursos educacionais disponíveis para apoiar esse processo ainda são limitados. Soma-se a esse cenário a formação ainda insuficiente dos profissionais da educação básica no ensino de temas relacionados à cibersegurança. Essa dificuldade decorre, entre outros fatores, da necessidade de preparar os docentes para lidar com os desafios impostos pela crescente digitalização da educação (BRASIL - Ministério da Educação, 2022). Como consequência, muitos professores têm dificuldades em integrar conteúdos de cibersegurança às suas práticas pedagógicas.

A revisão da literatura revela projetos que discutem a importância da cibersegurança nos dias atuais, mas ainda há espaço para avanços, especialmente no campo da educação digital. Jogos educacionais que abordam essa temática são escassos e, na maioria das vezes, focam em aspectos técnicos, frequentemente direcionados a usuários com conhecimentos prévios. Embora esses aspectos sejam importantes e relevantes, muitas vezes se esquece de considerar os aspectos humanos, que são peças fundamentais para evitar perigos como a engenharia social (NG; HASAN, 2025). Isso abre oportunidades para explorar

diferentes dimensões da cibersegurança.

Torna-se necessária a investigação de recursos educacionais que possam apoiar o trabalho docente na abordagem de conteúdos de cibersegurança durante a educação básica. Além do desenvolvimento dessas ferramentas, é igualmente importante avaliar sua aplicação em contextos reais de ensino, produzindo evidências sobre seu potencial para favorecer a aprendizagem, ampliar a conscientização dos estudantes e subsidiar futuras iniciativas na área de Informática na Educação.

Diante desse contexto, este trabalho apresenta um estudo empírico constituído pelo desenvolvimento e pela aplicação de um jogo digital educacional, voltado para a conscientização de estudantes do Ensino Fundamental I e II sobre os riscos associados à cibersegurança. O jogo foi concebido como uma ferramenta pedagógica de apoio à conscientização em cibersegurança, incorporando desafios relacionados ao uso de senhas fortes, à identificação de e-mails de *phishing*, ao reconhecimento de sites e arquivos maliciosos e à importância da realização periódica de *backups* de dados. A proposta busca contribuir com o desenvolvimento de recursos educacionais voltados à educação digital e produzir evidências sobre seu potencial como ferramenta de apoio ao processo de ensino e aprendizagem.

1.3 Objetivos e Desafios da Pesquisa

Apesar da crescente necessidade de educação em cibersegurança, promover a conscientização de crianças e adolescentes sobre os riscos digitais continua sendo um desafio relevante. Temas como privacidade, proteção de dados, golpes virtuais e engenharia social frequentemente são percebidos como abstratos ou distantes da realidade dos estudantes, o que dificulta seu ensino por meio de abordagens tradicionais. Somam-se a isso as diferenças de faixa etária, de maturidade cognitiva e de níveis de letramento digital presentes na educação básica. Diante desse contexto, torna-se necessário explorar estratégias pedagógicas mais interativas e alinhadas ao cotidiano dos estudantes, capazes de estimular o engajamento e favorecer a compreensão de conceitos fundamentais de segurança digital.

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é promover o aprendizado de cibersegurança entre estudantes do ensino básico, por meio do desenvolvimento e da avaliação de um jogo digital educacional que, com uma abordagem lúdica e acessível, estimule a compreensão e a aplicação de práticas seguras no ambiente virtual.

1.3.2 Objetivos Específicos

Para alcançar o objetivo geral proposto, foram estabelecidos três objetivos específicos que orientam o desenvolvimento, a implementação e a avaliação do jogo Encrypta. Esses objetivos são apresentados a seguir:

- ❏ Realizar um estudo comparativo de propostas da literatura relacionadas ao ensino de cibersegurança por meio de jogos digitais, visando identificar requisitos para a proposta deste trabalho;
- ❏ Desenvolver um jogo digital educacional destinado a estudantes do ensino básico para apoiar o aprendizado de cibersegurança.
- ❏ Conduzir um estudo empírico com estudantes do ensino básico para avaliar a usabilidade, a experiência dos jogadores e o aprendizado em cibersegurança proporcionados pelo jogo.

1.3.3 Questões de Pesquisa

Com o intuito de orientar a investigação e delimitar os aspectos analisados nesta pesquisa, foram definidas duas *Research Questions* (RQs). Essas questões de pesquisa foram elaboradas a partir do objetivo geral e dos objetivos específicos deste trabalho, direcionando a condução do estudo e a análise dos resultados obtidos.

- ❏ **RQ1:** Em que medida a utilização de um jogo digital educacional sobre práticas de cibersegurança pode favorecer a aprendizagem de estudantes do ensino básico sobre riscos associados ao ambiente virtual e como os estudantes percebem sua própria aprendizagem?
  - **RQ1.1:** Quais diferenças no desempenho e na aprendizagem percebida são observadas em função do sexo, da série escolar e da idade dos participantes após a utilização do jogo?
- ❏ **RQ2:** Como os elementos lúdicos presentes no jogo se relacionam com a motivação e o engajamento percebidos ou observados durante a interação dos participantes com a ferramenta?

Com base nas RQs definidas neste estudo, apresentam-se, a seguir, as estratégias adotadas para responder a cada uma delas.

- ❏ **RQ1:** Foi investigada por meio da aplicação de testes de conhecimento antes e após a interação com o jogo, com o objetivo de avaliar possíveis mudanças no conhecimento dos participantes sobre os conteúdos de cibersegurança. Complementarmente, foram

consideradas as percepções dos estudantes acerca da aprendizagem por meio das dimensões correspondentes do método MEEGA+.

  - **RQ1.1:** Os resultados obtidos para a RQ1 foram estratificados de acordo com características dos participantes, como sexo, faixa etária e série escolar, permitindo analisar possíveis diferenças entre os grupos. Essa análise considerou tanto os resultados objetivos dos testes de conhecimento quanto a percepção de aprendizagem obtida pelo MEEGA+.

- **RQ2:** Foi investigada por meio da análise dos registros (*logs*) da aplicação, da observação direta dos participantes e das dimensões avaliadas pelo método MEEGA+, buscando compreender aspectos relacionados à motivação e ao engajamento durante a interação com o jogo. Para a análise dos aspectos associados à motivação, foram consideradas as dimensões Confiança, Relevância e Satisfação avaliadas pelo MEEGA+, por apresentarem correspondência com componentes motivacionais do modelo ARCS (KELLER, 1987). Os aspectos relacionados ao engajamento foram analisados por meio das dimensões Atenção Focada, Diversão, Desafio e Interação Social, avaliadas pelo MEEGA+, considerando sua relação com a perspectiva multidimensional de engajamento proposta por Fredricks, Blumenfeld e Paris (2004) e com as características da experiência de fluxo descritas por Csikszentmihalyi (1990).

1.4 Contribuições

As contribuições deste projeto se estendem para além do campo educacional, alcançando também os âmbitos social e científico. Do ponto de vista educacional, o desenvolvimento de um jogo digital voltado à conscientização em cibersegurança favorece a aprendizagem de crianças e adolescentes, por meio de uma abordagem lúdica e interativa que estimula o engajamento e a retenção de conhecimentos.

1.4.1 Contribuições Práticas

- Um jogo digital educacional voltado para crianças e adolescentes da educação básica, com foco na conscientização sobre cibersegurança, disponibilizado gratuitamente para toda a comunidade;

- Contribuição para a implementação das competências relacionadas à segurança digital previstas na BNCC, oferecendo um recurso educacional que pode apoiar docentes na inserção desses conteúdos no contexto da educação básica.

1.4.2 Contribuições Científicas

- ❑ Investigação empírica das mudanças observadas no desempenho em testes de conhecimento e na percepção dos estudantes após a utilização de um jogo digital educacional sobre cibersegurança;
- ❑ Publicação dos resultados em eventos científicos da área.

1.4.3 Contribuições Sociais

- ❑ Promoção do ganho de conhecimento de estudantes do ensino básico sobre riscos e boas práticas no uso da internet;
- ❑ Estímulo para que os estudantes se tornem agentes multiplicadores de conhecimento sobre segurança digital em seus ambientes sociais.

1.5 Organização da Dissertação

Esta dissertação está estruturada em sete capítulos, descritos a seguir:

- ❑ **Capítulo 1: Introdução** - Contextualiza o tema, define os objetivos do trabalho, destaca as contribuições, apresenta as questões científicas e descreve a organização da dissertação.
- ❑ **Capítulo 2: Fundamentação Teórica** - Discute os conceitos essenciais para a compreensão do tema, incluindo educação digital, segurança cibernética e jogos educacionais como estratégia de conscientização.
- ❑ **Capítulo 3: Trabalhos Correlatos** - Analisa estudos que utilizaram jogos digitais educacionais como ferramenta para o aprendizado em cibersegurança.
- ❑ **Capítulo 4: Método** - Descrever o método adotado no desenvolvimento e na execução do estudo, abordando a problemática, o *design* e a implementação do jogo digital, bem como a análise dos dados obtidos na aplicação.
- ❑ **Capítulo 5: *Design* e Implementação do Jogo Encrypta** - Apresenta a narrativa do jogo, os tópicos de cibersegurança abordados em cada fase, bem como as ferramentas de desenvolvimento utilizadas.
- ❑ **Capítulo 6: Análise dos Resultados e Discussões** - Apresenta os resultados obtidos e os discute com base nos objetivos propostos nesta pesquisa.
- ❑ **Capítulo 7: Conclusão** - Sintetiza os principais resultados obtidos na pesquisa, enfatiza as contribuições do estudo e sugere direções para trabalhos futuros.

Capítulo 2

Fundamentação Teórica

Este capítulo apresenta os principais fundamentos teóricos que sustentam o desenvolvimento desta pesquisa. Inicialmente, são discutidos conceitos relacionados à Educação Digital, destacando sua evolução, seus princípios e sua importância na formação de cidadãos capazes de atuar de forma crítica, ética e segura em ambientes digitais, além de apresentar os fundamentos teóricos e pedagógicos que justificam o uso de jogos digitais educacionais como estratégia para promover a aprendizagem e a conscientização em cibersegurança, bem como o potencial desses jogos para estimular o engajamento, a participação ativa e o desenvolvimento de competências relacionadas à segurança no ambiente virtual. Em seguida, são abordados aspectos da Segurança Cibernética, com ênfase nos riscos aos quais crianças e adolescentes estão expostos durante o uso da internet e na relevância da conscientização em segurança digital no contexto da educação básica.

2.1 Educação Digital

A educação constitui-se como um processo essencial para o desenvolvimento integral do ser humano, contemplando dimensões físicas, psicomotoras, sociais, morais e intelectuais, entre outras. Garantida como um direito de todos pelo estado, a educação tem como finalidade a formação do indivíduo tanto para o exercício da cidadania quanto para a qualificação para o trabalho (MONTE; NOVAIS, 2024).

No modelo tradicional de ensino, o processo de aprendizagem é centrado no professor, que assume o papel de principal transmissor do conhecimento. Nesse contexto, os estudantes são expostos aos conteúdos das disciplinas por meio de recursos como o quadro negro e os livros didáticos. Tal abordagem caracteriza-se pela passividade do estudante no processo educativo, resultando em pouca ou nenhuma interação entre estudantes e educadores. Essa limitação restringe as formas de construção do conhecimento e pode comprometer o engajamento e a motivação dos educandos (FONSECA et al., 2025).

2.1.1 Educação 5.0

Ao longo dos anos, a educação passou por diversas transformações, evoluindo em direção ao que se propõe como Educação 5.0, um modelo educacional que busca integrar tecnologias digitais, valores humanos e personalização do ensino. Antes dela, surgiram os modelos 1.0, 2.0, 3.0 e 4.0. A Educação 1.0 era baseada no ensino cristão, tendo o professor como figura central e o estudante como sujeito passivo, cuja função era apenas receber o conhecimento transmitido. Já a Educação 2.0 surgiu com a Revolução Industrial e tinha como objetivo preparar indivíduos para trabalhar nas indústrias, por meio de tarefas mecânicas e repetitivas. Assim, o estudante continuava sem voz ativa, e o erro era visto como algo a ser evitado a todo custo (FELCHER; FOLMER, 2021).

A partir da Educação 3.0, os estudantes passaram a ter maior protagonismo, e o erro passou a ser compreendido como parte essencial do processo de aprendizagem. Essa fase marcou o início da integração das tecnologias digitais ao ensino, incentivando seu uso em sala de aula. A Educação 4.0, por sua vez, evoluiu esse conceito ao alinhar o aprendizado com as inovações tecnológicas, defendendo a ideia de *learning by doing*, ou seja, aprender fazendo, enfatizando a prática como meio de consolidar o conhecimento, colocando a tecnologia como parte central do processo de ensino (FELCHER; FOLMER, 2021).

Por fim, a Educação 5.0 representa uma evolução dos modelos educacionais anteriores ao recolocar o ser humano no centro do processo de aprendizagem. Essa abordagem integra tecnologias digitais de forma consciente ao ensino, não apenas para promover a aquisição de conhecimentos acadêmicos, mas também para favorecer o desenvolvimento integral dos estudantes. Nesse contexto, são valorizadas as competências socioemocionais e as *soft skills*, como trabalho em equipe, empatia, pensamento analítico e resolução de problemas. Além disso, a Educação 5.0 propõe uma reflexão sobre os impactos da tecnologia na mente humana, buscando compreender como os indivíduos aprendem, interagem e se desenvolvem em ambientes digitais (FILHO et al., 2025; ROMÃO et al., 2025).

2.1.2 Tecnologia como Suporte na Aprendizagem

O uso da tecnologia como ferramenta de apoio ao aprendizado humano constitui um importante elemento para o desenvolvimento pessoal e profissional dos estudantes. As metodologias associadas à Educação 5.0 promovem um ambiente inclusivo e personalizado, adaptável aos diferentes perfis de individuos, graças à ampla variedade de recursos tecnológicos disponíveis. Esse modelo estimula uma aprendizagem colaborativa, engajante e motivadora, oferecendo acesso a ferramentas lúdicas e acessíveis que favorecem o processo de ensino. Dessa forma, o estudante é reconhecido como o centro do processo de aprendizagem, assumindo um papel ativo em seu desenvolvimento, enquanto o professor deixa de ser um transmissor de conhecimento para atuar como mediador e facilitador da construção do saber (ROMÃO et al., 2025).

De acordo com Teixeira (2023), o uso de dispositivos digitais é incentivado desde os primeiros anos de vida, expondo usuários, ainda na infância, aos riscos e ameaças do ambiente virtual. A educação digital assume um papel fundamental ao proporcionar orientações que favoreçam uma relação mais saudável, segura e ética com as tecnologias.

Assim, a educação digital apresenta uma ampla gama de possibilidades pedagógicas. O uso de mídias digitais, como jogos eletrônicos e plataformas interativas, amplia as formas de acesso ao conhecimento e favorece a inclusão dos estudantes. Diferentemente do modelo tradicional, a educação digital promove maior interação entre estudantes e professores, estimulando a participação ativa dos discentes nas atividades de aprendizagem. Essa abordagem contribui para o desenvolvimento de práticas colaborativas, o fortalecimento do engajamento e o aumento da motivação dos estudantes (FONSECA et al., 2025).

Com o advento da pandemia de Covid-19, a educação digital consolidou-se como um componente operacional essencial, especialmente no contexto do ensino remoto e dos modelos híbridos, que combinam os benefícios do aprendizado a distância com as interações presenciais tradicionais. Plataformas e ambientes virtuais de aprendizagem, como Google Classroom, Zoom e Microsoft Teams, tornaram-se fundamentais para garantir a continuidade das atividades escolares em um período em que o ensino presencial não era viável por razões de saúde pública.

Essas tecnologias possibilitam a organização de conteúdos, a comunicação entre professores e estudantes e o acompanhamento individualizado do desempenho. Nesse contexto, a alfabetização digital tornou-se ainda mais relevante, pois vai além do simples domínio de ferramentas tecnológicas, promovendo seu uso de forma crítica, ética e responsável (ZANOTTI, 2025). Essa perspectiva exige o desenvolvimento de competências técnicas, éticas, morais e sociais que permitam aos indivíduos compreender e atuar de maneira consciente em uma sociedade cada vez mais conectada (VASCONCELOS; PRADO; BARBIERI, 2023). Além de potencializar oportunidades de aprendizagem e interação, o ambiente digital também expõe seus usuários a riscos e ameaças decorrentes do uso inadequado da tecnologia ou da atuação de agentes mal-intencionados. Dessa forma, torna-se fundamental preparar os indivíduos não apenas para utilizar recursos digitais, mas também para reconhecer vulnerabilidades, adotar práticas seguras e proteger informações e sistemas. Nesse cenário, a segurança cibernética emerge como um elemento essencial da formação digital contemporânea.

2.1.3 Jogos Digitais Educacionais como Estratégia de Conscientização

De acordo com Ovigli et al. (2025), os jogos digitais configuram-se como ferramentas que atuam não apenas no desenvolvimento cognitivo e no processo de ensino e aprendizagem, mas também em aspectos emocionais que devem ser considerados no contexto

educacional. Os jogos digitais educacionais, tradicionalmente desenvolvidos com finalidades pedagógicas, são reconhecidos como instrumentos fundamentais para a mediação do conhecimento, contribuindo para um aprendizado mais dinâmico e interativo.

Para além de seu caráter lúdico, os jogos digitais consolidaram-se historicamente como uma das formas mais difundidas de entretenimento, mantendo sua relevância até os dias atuais (OVIGLI et al., 2025). No entanto, seu valor vai além do entretenimento. A incorporação dos jogos ao contexto educacional evidencia seu potencial como ferramenta didática, especialmente quando considerada à luz de fundamentos teóricos consolidados.

A utilização de jogos como recurso pedagógico dialoga com pressupostos teóricos consolidados, tais como Piaget (1976), que destaca o papel do jogo como uma forma essencial de construção do conhecimento durante o desenvolvimento cognitivo; Vygotsky (1991) que enfatiza a importância da interação social e do uso de instrumentos culturais (e.g. jogos e *games*) no processo de aprendizagem, ao mediar o desenvolvimento por meio da zona de desenvolvimento proximal; e, ainda complementando essas abordagens, Papert (1980) defende o uso de tecnologias digitais como ambientes de aprendizagem ativa, configurando a Educação Digital, onde os estudantes constroem conhecimento por meio da resolução de problemas reais.

Nesse sentido, os jogos educativos contribuem para a criação de ambientes de aprendizagem mais ativos, participativos e significativos, favorecendo tanto o engajamento dos estudantes quanto a internalização de conteúdos por meio da experiência lúdica.

Dentro desse contexto, em que os jogos digitais são utilizados como instrumentos para promover a conscientização e o aprendizado, especialmente em temas sensíveis como a cibersegurança, Bedwell et al. (2012) propõe nove pilares fundamentais que orientam o *design* e a construção de experiências lúdicas eficazes. Esses elementos estruturantes contribuem para o engajamento dos jogadores, favorecendo a imersão, a aprendizagem ativa e a internalização de comportamentos desejados, conforme ilustra a Tabela 1.

Tabela 1 – Pilares fundamentais na construção de jogos.

Pilar	**Descrição**
Linguagem de ação	Modo de interação do jogador com a interface e os controles do jogo, dependendo do *design* e gênero.
Avaliação	*Feedback* contínuo fornecido ao jogador, como pontuações, progresso e vidas restantes.
Desafios/Conflito	Obstáculos a serem superados pelo jogador, exigindo resolução ativa para avançar.
Controle	Grau de autonomia do jogador sobre suas ações e decisões estratégicas.
Ambiente	Cenário e ambientação que contextualizam os desafios e eventos do jogo.
Interação humana	Colaboração ou competição entre jogadores, conforme as regras do jogo.
Contexto/Ficção	Narrativa que dá sentido às ações do jogador e estrutura os desafios.
Regras/Objetivos	Diretrizes e metas que delimitam o funcionamento e o progresso no jogo.
Imersão	Envolvimento emocional e cognitivo do jogador, promovido pela coerência narrativa e ambientação.

Fonte: Adaptado de (BEDWELL et al., 2012).

Quando inseridos no contexto educacional, os jogos digitais podem apresentar inúmeras vantagens, como o aumento da motivação dos estudantes, o estímulo à interação social e a facilitação na assimilação de conteúdos. Além disso, podem favorecem a troca de experiências e o compartilhamento de conhecimentos entre os estudantes, fortalecendo o aprendizado em grupo (FURTADO; SOTIL, 2024; COELHO; COSTA; VALENTE, 2023).

Ante o exposto, torna-se importante ressaltar que, essas ferramentas devem ser avaliadas quanto à sua usabilidade e eficácia pedagógica antes de sua adoção em contextos formais de ensino. Além disso, é essencial que os docentes responsáveis pela mediação dessas atividades estejam devidamente preparados, tanto em relação ao domínio das funcionalidades do jogo quanto aos conteúdos a serem trabalhados, de modo a potencializar os benefícios dessa abordagem educativa (SCHÜNEMANN; GARCIA, 2023).

2.2 Segurança Cibernética

Com a popularização da internet, observa-se um crescimento exponencial no volume de dados compartilhados em ambientes digitais. De acordo com Cabral e Figueiredo (2025), esse cenário de conectividade constante propicia oportunidades para a atuação de cibercriminosos[1], que se aproveitam das vulnerabilidades presentes em dispositivos e comportamentos inseguros dos usuários. O aumento do acesso a redes sociais e plataformas digitais tem exposto os indivíduos a riscos crescentes relacionados à exposição de informações pessoais, fraudes digitais e golpes de engenharia social.

A cibersegurança pode ser compreendida como o conjunto de práticas, políticas e tecnologias destinadas à proteção de redes, sistemas e dados digitais, garantindo a confidencialidade, a integridade e a disponibilidade das informações. Sua relevância cresce diante do aumento dos cibercrimes[2] e da constante evolução das ameaças virtuais. Nesse contexto, a segurança digital deve ser entendida como um processo contínuo que envolve tanto a proteção da infraestrutura tecnológica quanto a conscientização dos usuários, buscando reduzir vulnerabilidades técnicas e humanas e promover um ambiente digital mais seguro (SOUZA et al., 2025b).

Os cibercriminosos utilizam diferentes estratégias para realizar atividades ilícitas no ambiente digital, sendo frequentemente classificados como *crackers*, *phishers*, *cyberstalkers*, entre outros (INAGAKI, 2023). Suas ações costumam atingir usuários vulneráveis, especialmente crianças e adolescentes, expostos a práticas como *cyberbullying*, assédio virtual, pornografia infantil e outros delitos digitais (INAGAKI, 2023).

Segundo Corrêa, Silva et al. (2023), os crimes cibernéticos podem ser divididos em duas categorias: os impróprios, cuja ocorrência não depende da tecnologia, embora possa ser facilitada por ela, e os próprios, que exigem o uso de recursos digitais e da internet para sua execução. A Tabela 2 ilustra essa organização.

[1] Indivíduos que utilizam a tecnologia para cometer crimes no ambiente virtual.

[2] Infrações cometidas por meio de computadores ou dispositivos com o objetivo de roubar informações, fraudar sistemas ou atacar vítimas.

Tabela 2 – Classificação dos crimes cibernéticos.

Crimes Cibernéticos Abertos/Impróprios	**Crimes Cibernéticos Exclusivamente Próprios**
✓ Crimes contra a honra	✓ Invasão de dispositivo informático mediante violação de segurança
✓ Ameaça	✓ Interceptação telemática ilegal
✓ Estelionato	✓ Pornografia infantil via informática
✓ Furto mediante fraude	✓ Corrupção de menores em sala de bate-papo
✓ Racismo	✓ Crimes contra a urna eletrônica
✓ Apologia ao crime	
✓ Falsa identidade	
✓ Concorrência desleal	
✓ Tráfico de drogas	

Fonte: Adaptado de (CORRÊA; SILVA et al., 2023).

A compreensão destas definições de crimes cibernéticos, os perfis dos agentes envolvidos e as vulnerabilidades exploradas constituem um elemento essencial para a formulação de estratégias educativas eficazes voltadas à prevenção dessas práticas ilícitas.

2.2.1 Segurança Cibernética no Ensino Básico

A segurança cibernética no ensino básico é um tema cada vez mais relevante diante do crescente acesso das crianças e adolescentes à internet. Observa-se que os estudantes dessa faixa etária estão expostos a diversos tipos de riscos digitais, entre os quais se destacam o *cyberbullying*, a engenharia social e a dificuldade em exercer uma análise crítica sobre as informações disponíveis no ambiente virtual. Essa falta de discernimento compromete a capacidade de identificar conteúdos confiáveis e de desenvolver um raciocínio crítico capaz de lidar com as diferentes ameaças às quais estão vulneráveis (JUNIOR, 2024).

Abordagens pedagógicas baseadas em gamificação têm se mostrado promissoras para a conscientização em cibersegurança entre estudantes do ensino básico. Essa estratégia aproxima os estudantes de situações reais, permitindo que compreendam de forma prática os riscos presentes no uso cotidiano da internet. Os jogos educacionais contribuem, assim, para um aprendizado ativo, participativo e envolvente, favorecendo o desenvolvimento da consciência digital e de comportamentos seguros no ambiente online (JUNIOR, 2024).

Conforme Perdiz e Neto (2025), um estudo sobre segurança digital entre crianças e adolescentes teve como objetivo identificar os principais crimes cibernéticos que afetam esse público, entre os quais destacam-se o *cyberbullying*, a exploração sexual e a engenharia social. Os autores ressaltam que o impacto dessas práticas pode levar à evasão escolar, depressão, isolamento social e, em casos mais graves, suicídio, evidenciando a gravidade das ameaças às quais crianças e adolescentes estão expostos no ambiente virtual.

Adicionalmente, ao analisar as diretrizes da BNCC, observa-se um direcionamento progressivo para a conscientização em temas de cibersegurança desde os anos iniciais (BRASIL - Ministério da Educação, 2022). No 4º ano, a habilidade EF04CO08 já estabelece a importância de os estudantes verificarem a confiabilidade das informações obtidas na rede. Para os 5º e 6º anos, as habilidades EF05CO06 e EF06CO08 introduzem o ensino sobre sistemas de armazenamento de arquivos, enquanto a EF05CO08 reforça a necessidade de distinguir conteúdos confiáveis de fontes inseguras. No 7º ano, a diretriz EF07CO07, consolida os fundamentos de segurança cibernética, com o objetivo de elucidar os mecanismos de proteção essenciais no ambiente online.

Com base no exposto, embora a área de cibersegurança seja ampla, este trabalho delimita seu escopo a temas relacionados à segurança digital e à engenharia social, tópicos recomendados pela BNCC e adequados ao contexto educacional do ensino básico. Nesse sentido, o jogo desenvolvido aborda os seguintes eixos: o uso de senhas fortes, a detecção de tentativas de *phishing* e de sites maliciosos, a importância da realização de *backups* e a identificação de arquivos potencialmente maliciosos.

Esta proposta propõe a utilização de jogos digitais como instrumento pedagógico voltado à promoção do aprendizado e ao desenvolvimento de competências em segurança digital, com foco em públicos particularmente vulneráveis, como crianças e adolescentes, principalmente no contexto da educação básica. Ao incorporar conceitos referentes à natureza, à classificação e às implicações dos crimes cibernéticos, este trabalho objetiva não apenas favorecer a compreensão desses conteúdos, mas também contribuir para a conscientização dos estudantes sobre as principais ameaças presentes no ciberespaço por meio de um jogo digital educacional.

Diante dos aspectos apresentados, torna-se necessário analisar como esses fundamentos têm sido aplicados em pesquisas e soluções existentes voltadas ao ensino de cibersegurança por meio de jogos digitais educacionais. A investigação de trabalhos correlatos permite identificar as principais abordagens adotadas na literatura, bem como suas contribuições e limitações, possibilitando compreender as lacunas ainda presentes na área e orientar o desenvolvimento da proposta apresentada nesta dissertação.

Capítulo 3

Trabalhos Correlatos

Esta seção apresenta os principais trabalhos sobre o uso de jogos digitais educacionais no ensino e na conscientização em cibersegurança. Inicialmente, são discutidos estudos de revisão da literatura que investigam o estado da arte da área e identificam desafios recorrentes na concepção, implementação e avaliação dessas ferramentas. Em seguida, são analisados jogos digitais desenvolvidos com o propósito de ensinar conceitos de segurança digital a diferentes públicos, destacando suas características, estratégias pedagógicas e métodos de validação. Por fim, realiza-se uma análise comparativa dos trabalhos identificados, evidenciando lacunas e oportunidades de pesquisa que fundamentam o desenvolvimento da proposta apresentada nesta dissertação.

3.1 Panorama da Literatura e Lacunas de Pesquisa

Diversos estudos de revisão têm investigado o uso de jogos educacionais como estratégia para promover a conscientização e o aprendizado em cibersegurança. Esses trabalhos analisam diferentes abordagens, métodos de avaliação e públicos-alvo, permitindo identificar desafios recorrentes e lacunas ainda existentes na área.

Ferreira et al. (2024) apresentam uma revisão sistemática da literatura sobre jogos sérios voltados ao combate ao *phishing*. Os autores destacam que a maioria dos trabalhos revisados realiza testes em universidades onde os jogos foram desenvolvidos ou com funcionários de empresas e de setores de tecnologia. Essa escolha tende a incluir participantes com conhecimento prévio em tecnologia, o que pode influenciar os resultados, uma vez que esses indivíduos possivelmente possuem noções básicas de cibersegurança. Adicionalmente, a revisão da literatura evidencia que muitos estudos não detalham adequadamente os resultados de aprendizagem obtidos na etapa de validação, o que caracteriza uma lacuna importante a ser preenchida. Outro ponto observado é a ausência de padrão na coleta de *feedback* dos usuários, o que dificulta a compreensão da percepção e das preferências dos jogadores.

Em Amjad et al. (2025), os autores analisaram estudos sobre jogos sérios aplicados à

cibersegurança e identificaram falhas recorrentes. Os autores destacam que grande parte das pesquisas utiliza ferramentas insuficientes para medir a aprendizagem, concentrando-se apenas em avaliações pós-jogo, o que impede inferências precisas sobre o ganho real de conhecimento. Com isso, pode-se observar o predomínio de métodos quantitativos simples ou qualitativos que, por dependerem de autoavaliações, ficam vulneráveis a erros humanos ou respostas desonestas por parte dos participantes.

A pesquisa conduzida por Gwenhure e Rahayu (2024) analisou estratégias de gamificação para promover a conscientização em cibersegurança entre públicos não especializados em tecnologia. A análise revela que a maioria dos trabalhos avalia suas ferramentas de forma predominantemente qualitativa, o que é útil para captar o *feedback* dos usuários, mas suscetível a vieses subjetivos. Além da importância das avaliações qualitativas, os autores ressaltam a necessidade de empregar abordagens quantitativas mais objetivas, baseadas em dados numéricos, para garantir resultados mais claros e cientificamente robustos. Outra lacuna identificada por este estudo é a escassez de estudos validados com estudantes e profissionais não pertencentes à área de tecnologia da informação, considerados o público mais vulnerável a ataques cibernéticos.

Na revisão sistemática apresentada por Ng e Hasan (2025), que abordou jogos sérios desenvolvidos para a educação em cibersegurança, os autores observaram que a maioria desses jogos é direcionada a públicos já familiarizados com segurança cibernética, como estudantes ou profissionais de tecnologia, o que limita a avaliação da eficácia, uma vez que esses indivíduos já possuem conhecimento prévio. Além disso, constatou-se uma escassez de abordagens relacionadas à engenharia social, com foco predominante em tópicos técnicos, como *hacking* e arquitetura de redes.

Por fim, em Damenu et al. (2025), os autores revisam estudos sobre jogos educacionais de cibersegurança desenvolvidos para crianças. Neste estudo, os autores apontam que a maioria dos jogos não é disponibilizada ao público após a fase de testes, permanecendo apenas em protótipo e, em poucos casos, chegando a ser disponibilizados. Outra lacuna relevante refere-se à falta de diversidade entre os participantes dos testes, sendo comum a ausência de informações demográficas (idade, gênero, escolaridade) ou a restrição a grupos homogêneos.

Ainda de acordo com Damenu et al. (2025), os autores destacam também que muitos estudos não realizam testes com crianças, optando por adolescentes, mesmo quando o público-alvo declarado são as próprias crianças. Por fim, os autores ressaltam a carência de fundamentação teórica e de *frameworks* educacionais para orientar o *design*, a implementação e a avaliação dos jogos, evidenciando a ausência de modelos teóricos amplamente aceitos.

Em síntese, os estudos analisados demonstram o potencial dos jogos digitais como ferramenta de apoio à educação em cibersegurança, mas também revelam limitações metodológicas e pedagógicas que ainda precisam ser superadas. Questões relacionadas à

avaliação da aprendizagem, à diversidade dos participantes, à fundamentação educacional e à abrangência dos conteúdos permanecem como desafios relevantes, indicando oportunidades para o desenvolvimento de soluções mais efetivas e adequadas ao contexto da educação básica.

3.2 Jogos Digitais em Cibersegurança

A partir das lacunas evidenciadas pelas revisões apresentadas, foi conduzida uma pesquisa exploratória, seguindo os princípios metodológicos propostos por Marconi e Lakatos (2004), com o propósito de identificar jogos digitais educacionais voltados ao ensino de cibersegurança. A análise desses estudos permitiu examinar suas características, estratégias pedagógicas e métodos de avaliação, bem como identificar limitações que serviram de subsídio ao desenvolvimento da proposta apresentada nesta dissertação.

3.2.1 Aprendendo Segurança da Informação

O jogo digital apresentado por Frydman e Bueno (2023), denominado "Aprendendo Segurança da Informação", é estruturado sob a mecânica de jogos do tipo *Role-Playing Game* (RPG)[1], na qual o jogador assume o papel de funcionário de uma empresa. Ao longo de cinco fases, o usuário pode explorar diferentes ambientes virtuais e interagir com personagens do cenário. Em cada etapa, são introduzidos conceitos fundamentais relacionados à segurança da informação, tais como a proibição do uso de dispositivos de armazenamento removíveis no ambiente corporativo, os riscos associados à divulgação de imagens que revelem dados institucionais, bem como orientações sobre o manuseio de informações sensíveis e o reconhecimento de e-mails e sites fraudulentos (FRYDMAN; BUENO, 2023). Para validar a aplicação, os autores não utilizaram métodos tradicionais de avaliação, como questionários de usabilidade, análise da experiência do usuário ou testes de aprendizado. Em vez disso, a avaliação foi realizada por meio da análise de *logs* do banco de dados da aplicação e da coleta de interações de usuários em postagens na rede social Linkedin, permitindo identificar as reações e o engajamento dos usuários alcançados. A Figura 1 apresenta uma tela do jogo desenvolvido pelos autores.

[1] *Role-Playing Game* (RPG) é um tipo de jogo em que os participantes assumem a identidade de personagens fictícios e criam narrativas de forma colaborativa.

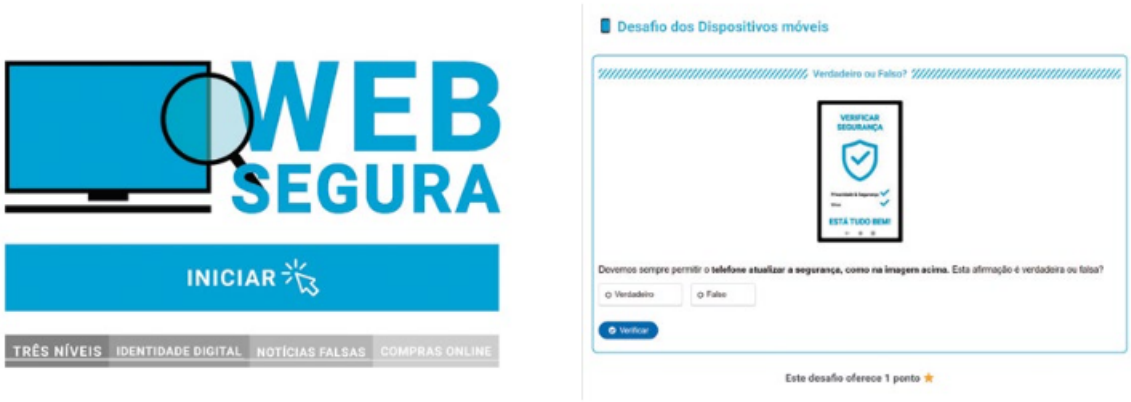
Figura 1 – Captura de tela do jogo “Aprendendo Segurança da Informação”.

Fonte: (FRYDMAN; BUENO, 2023).

3.2.2 Web Segura

O jogo digital sério desenvolvido por Bernardino et al. (2023), intitulado “Web Segura”, é apresentado com o intuito de alertar estudantes seniores sobre os perigos presentes na internet e ajudá-los a compreendê-los e enfrentá-los. Por meio de *quizzes* e minijogos interativos, a aplicação aborda questões relacionadas à segurança na internet, como o incentivo ao uso de senhas fortes, formas de detectar sites fraudulentos, identificar notícias falsas e cuidados em compras online. A avaliação da aplicação foi conduzida por meio de testes de usabilidade e satisfação, com o objetivo de coletar o *feedback* dos participantes. Entretanto, conforme destacado pelos autores, essa coleta foi realizada em um grupo reduzido, composto por apenas três indivíduos. A Figura 2 ilustra o jogo “Web Segura”.

Figura 2 – Captura de tela do jogo “Web Segura”.



Fonte: (BERNARDINO et al., 2023).

3.2.3 Alerta

O trabalho proposto por Júnior et al. (2024) apresenta o jogo digital intitulado “Alerta” com o objetivo de ensinar os jogadores a identificarem e distinguirem e-mails legítimos de

possíveis e-mails de *phishing*. Em testes conduzidos pelos autores, foi possível observar que o jogo alcançou os objetivos iniciais propostos, com os jogadores progredindo de forma orgânica e reconhecendo e-mails de *phishing* na maioria das situações apresentadas. Além disso, os testes de usabilidade realizados demonstraram uma resposta positiva por parte do público avaliado, indicando que a interface e a mecânica do jogo foram bem recebidas. Para realizar a avaliação da aplicação, os autores propuseram testes de usabilidade, satisfação e aprendizagem por meio de questionários de pré e pós-teste. Na Figura 3 é possível visualizar o jogo apresentado.

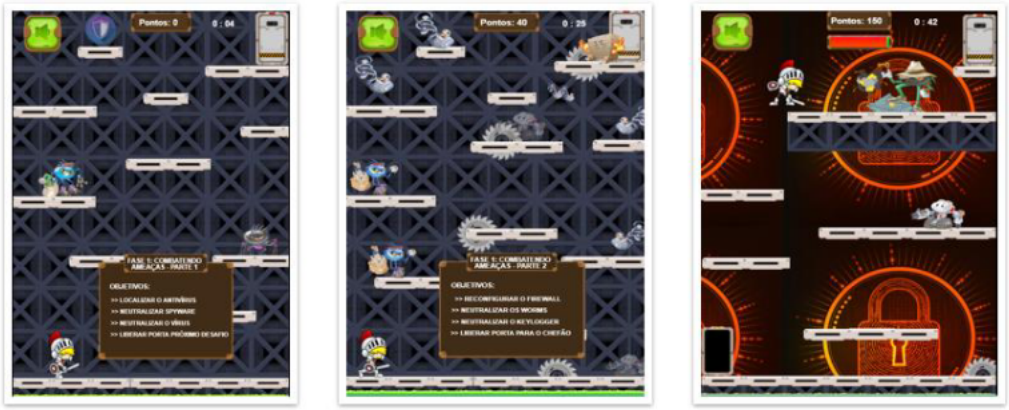
Figura 3 – Captura de tela do jogo "Alerta".

Fonte: (JÚNIOR et al., 2024).

3.2.4 Self Protect

No projeto apresentado por Farias et al. (2019), os autores introduzem o jogo "Self Protect", um *Jumping Game* em que os jogadores controlam um personagem que deve evitar ameaças como *worms*, *keyloggers*, *spywares* e *ransomwares*, sendo estas ameaças ferramentas frequentemente usadas por cibercriminosos para invadir sistemas, roubar dados ou prejudicar usuários. Além disso, os jogadores devem buscar itens de segurança, como antivírus e *firewalls*, que podem ajudá-los a neutralizar as ameaças presentes durante as fases. Os autores utilizaram questionários de satisfação como instrumento para a coleta dos resultados, aplicados a um grupo de noventa e nove estudantes que participaram dos testes. É possivel visualizar o jogo desenvolvido na Figura 4.

Figura 4 – Captura de tela do jogo “Self Protect”.

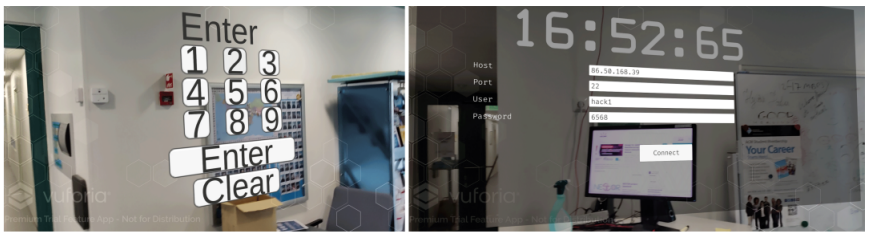


Fonte: (FARIAS et al., 2019).

3.2.5 Hack the Room

O projeto apresentado por Korkiakoski et al. (2023) retrata o “Hack the Room”, um jogo de realidade aumentada cujo objetivo é utilizar o telefone celular para escanear áreas do mundo real, onde elementos como computadores e teclados são sobrepostos virtualmente. Nesse contexto, os jogadores precisam interagir com esses elementos, utilizando comandos básicos de Linux para ler arquivos, encontrar senhas e códigos, a fim de avançar no jogo. O propósito do projeto é promover o ensino de cibersegurança e proporcionar uma experiência de *hacking* ético. Para a avaliação da aplicação, os autores consideraram dois perfis de jogadores: novatos e participantes com experiência prévia em cibersegurança, além de certo conhecimento em aplicações de realidade aumentada. A testagem foi realizada por meio de questionários distintos, sendo os de aprendizagem aplicados ao grupo de novatos e os de consciência situacional direcionados aos jogadores experientes. Além disso, os testes foram complementados por instrumentos de coleta de dados que avaliaram a experiência do usuário e a percepção da ferramenta durante o uso. A Figura 5 ilustra a interface do jogo.

Figura 5 – Captura de tela do jogo “Hack the Room”.



Fonte: (KORKIAKOSKI et al., 2023).

3.2.6 Cyber Defender

Já Santos et al. (2025) apresentam o jogo digital "Cyber Defender", um jogo educacional voltado para o ensino de segurança cibernética. Durante a experiência, os usuários podem se deslocar em um cenário fictício que simula um ambiente de escritório, interagindo com personagens dispostos no local. Como recompensa, são apresentados a diferentes minijogos, nos quais aprendem conceitos relacionados a *phishing*, *ransomware* e *Distributed Denial of Service* (DDoS). Para a avaliação do projeto, os autores recorreram a métodos consolidados na literatura, dentre os quais estão o modelo MEEGA+, IAQJEd, Pro-Avalia JS e PAJED, todos voltados para a análise da percepção e da experiência dos jogadores. Na Figura 6 é possível visualizar a interface do jogo proposto.

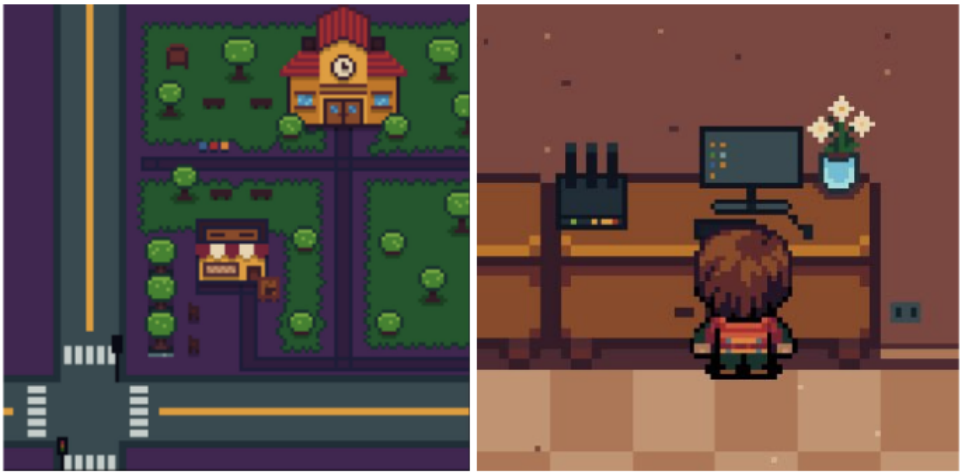
Figura 6 – Captura de tela do jogo "Cyber Defender".

Fonte: (SANTOS et al., 2025).

3.2.7 Cyber Resistance

"Cyber Resistance" é um protótipo apresentado por Souza et al. (2025a), no qual os autores desenvolveram um jogo digital educacional em que os jogadores assumem o papel de estudantes recém-ingressos na universidade. O objetivo é superar uma série de desafios enfrentando uma organização que controla o mundo por meio de tecnologias da informação. Ao longo da jornada, os jogadores não apenas aprendem conceitos relacionados à segurança cibernética, mas também desenvolvem conhecimentos sobre redes de computadores, lógica e programação. A avaliação da aplicação foi realizada por meio de questionários de percepção dos usuários, complementados pela análise das respostas de um *quiz* presente no jogo. A Figura 7 ilustra o jogo desenvolvido.

Figura 7 – Captura de tela do jogo “Cyber Resistance”.



Fonte: (SOUZA et al., 2025a).

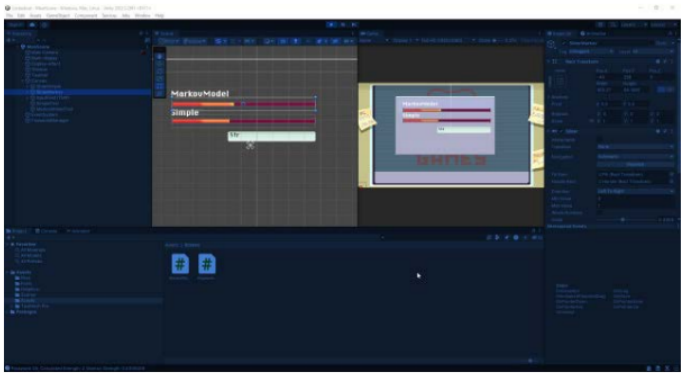
3.2.8 Quizzes Interativos

Dias et al. (2025) apresentam o uso de *quizzes* interativos como ferramenta de apoio à educação em cibersegurança. O projeto consistiu no desenvolvimento de atividades voltadas à identificação de diferentes tipos de golpes online, como fraudes relacionadas a empréstimos e perfis falsos que se passam por conhecidos, entre outras situações comuns no ambiente digital. Para avaliar os resultados, os autores utilizaram questionários destinados a analisar a percepção dos usuários sobre os conteúdos abordados, bem como o desempenho obtido na resolução dos *quizzes*.

3.2.9 Lockedout

No trabalho apresentado por Kostic e Saveljic (2024), os autores descrevem o jogo educacional “Lockedout”, cujo objetivo principal é incentivar o uso de senhas fortes. Na dinâmica do jogo, os participantes interagem com um computador virtual que sofre um ataque repentino, devendo agir rapidamente para alterar as senhas de diferentes aplicativos, como os de bancos, e-mail, mídias sociais e outras plataformas, a fim de impedir o ataque cibernético ao qual estão expostos. Para avaliar a aplicação, os autores realizaram testes de robustez comparando o desempenho de sua ferramenta com soluções de mercado. Além disso, utilizaram bases de dados externas de senhas vazadas para validar a eficácia técnica do sistema na detecção de credenciais fracas. No entanto, não foram apresentados testes com usuários finais para validar a experiência e o impacto educacional do jogo. A Figura 8 ilustra o protótipo desenvolvido.

Figura 8 – Captura de tela do jogo “Lockedout”.

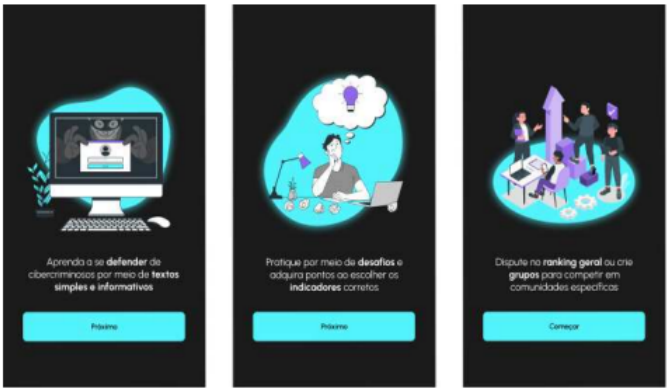


Fonte: (KOSTIC; SAVELJIC, 2024).

3.2.10 Saphish

Cardoso (2024) apresenta o jogo mobile “Saphish”, cujo objetivo principal é abordar questões relacionadas a *phishing* e engenharia social. Na aplicação, os jogadores podem interagir com diferentes tópicos, onde devem trabalhar para identificar e distinguir e-mails, mensagens de texto fraudulentas e até mesmo *Uniform Resource Locator* (URLs) de sites maliciosos. Para a avaliação do jogo, os autores aplicaram formulários com o intuito de coletar a percepção dos participantes a respeito da experiência proporcionada pela aplicação. A Figura 9 ilustra o protótipo desenvolvido.

Figura 9 – Captura de tela do jogo “Saphish”.



Fonte: (CARDOSO, 2024).

3.3 Síntese dos Trabalhos Correlatos

Os estudos analisados demonstram que os jogos digitais educacionais constituem uma estratégia promissora para a conscientização em cibersegurança, com potencial para apoiar a aprendizagem de conceitos relacionados à segurança digital e estimular comportamentos

mais seguros no ambiente virtual. Observa-se que muitas iniciativas ainda apresentam limitações metodológicas, especialmente no que diz respeito à avaliação sistemática da aprendizagem, da usabilidade e da experiência dos usuários.

Com o objetivo de sintetizar as características dos trabalhos analisados, a Tabela 3 apresenta uma comparação baseada em oito critérios (A a H), selecionados por sua relevância para a avaliação de jogos digitais educacionais voltados à cibersegurança. Os critérios contemplam aspectos pedagógicos, técnicos e de avaliação, permitindo uma análise mais abrangente das abordagens existentes. Essa comparação permite evidenciar lacunas ainda presentes na literatura e destacar elementos considerados no desenvolvimento da proposta apresentada nesta dissertação.

- **A. Aprendizado:** Refere-se à avaliação da eficácia pedagógica do jogo, isto é, à sua capacidade de promover a aquisição de conhecimentos em cibersegurança. Reconhece-se que abordagens que avaliam empiricamente a evolução do conhecimento, do entendimento prévio ao adquirido após a interação com a ferramenta, permitem mensurar o aprendizado de forma mais consistente.

- **B. Usabilidade:** Considera à facilidade de uso do jogo, abordando questões como intuitividade, eficiência nas interações e a facilidade de compreensão e navegação na ferramenta. Avalia a experiência do usuário em termos de praticidade e simplicidade.

- **C. Experiência do jogador:** Diz respeito à qualidade da interação do jogador com o jogo, incluindo aspectos como a experiência ao usar a ferramenta, a qualidade do *design* e a motivação para continuar jogando.

- **D. *Logs* do Jogo:** Refere-se aos trabalhos que utilizam os *logs* gerados pela ferramenta durante sua aplicação, permitindo analisar o comportamento e as interações dos usuários ao longo da atividade.

- **E. Multiplataforma:** Indica se o jogo pode ser jogado em diferentes plataformas (desktop, mobile, web, entre outras), oferecendo acessibilidade em diversos dispositivos.

- **F. Abrangência de Conteúdo:** Avalia o escopo dos tópicos abordados no jogo. Consideram-se abrangentes os jogos que abordam diversas áreas da cibersegurança, incluindo não apenas aspectos técnicos, mas também questões sociais relacionadas à segurança digital.

- **G. Personalização do Conteúdo:** Refere-se à capacidade do sistema em permitir que o docente adapte o conteúdo pedagógico de acordo com as necessidades da turma. Essa flexibilidade garante que o jogo permaneça relevante para diferentes perfis de jogadores e níveis de conhecimento.

- ❑ **H. Modo *Offline***: Indica a possibilidade de execução do jogo tanto em ambientes conectados à internet quanto de forma independente, considerando a acessibilidade para escolas e instituições com infraestrutura de rede limitada.

Tabela 3 – Comparação dos trabalhos correlatos.

TRABALHOS	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Web Segura (BERNARDINO et al., 2023)	-	X	X	-	-	X	-	-
Seg. da Informação (FRYDMAN; BUENO, 2023)	-	-	-	X	-	X	-	X
Alerta (JÚNIOR et al., 2024)	X	X	-	-	-	-	-	X
Self Protect (FARIAS et al., 2019)	-	-	X	-	-	-	-	-
Hack the Room (KORKIAKOSKI et al., 2023)	X	X	X	-	-	-	-	X
Cyber Defender (SANTOS et al., 2025)	-	X	X	-	X	X	-	X
Cyber Resistance (SOUZA et al., 2025a)	-	-	X	-	-	X	-	X
Quizzes Interativos (DIAS et al., 2025)	-	-	X	-	-	-	-	-
Password Checker (KOSTIC; SAVELJIC, 2024)	-	-	-	-	-	-	-	X
Saphish (CARDOSO, 2024)	-	-	X	-	-	-	-	X
Encrypta (Esta Dissertação)	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

Fonte: Elaboração própria.

Legenda: A: Aprendizado; **B:** Usabilidade; **C:** Exp. do Jogador; **D:** *Logs* do Jogo; **E:** Multiplataforma; **F:** Abrangência de Conteúdo; **G:** Personalização do Conteúdo; **H:** Modo *Offline*.

Com base nas informações apresentadas, este projeto tem como objetivo preencher as lacunas deixadas por esses estudos. Como observado nesta seção, os projetos analisados falham em apresentar resultados relacionados a questões de usabilidade e aprendizado da ferramenta, aspectos fundamentais para a validação de uma proposta educacional. Este projeto buscou fornecer *insights* completos sobre o aprendizado dos jogadores, a usabilidade e a satisfação dos usuários com o *software*. Além disso, focou em criar uma ferramenta acessível para diferentes públicos na esfera do ensino básico, com uma abrangência de conteúdo tanto técnico quanto social, proporcionando uma formação em cibersegurança mais completa aos usuários. Por fim, o jogo foi disponibilizado em diversos contextos multiplataforma.

Enquanto os trabalhos relacionados, em sua maioria, focaram prioritariamente em métodos tradicionais de avaliação, este trabalho ampliou essa análise ao integrar testes de aprendizado (pré e pós-teste) ao modelo MEEGA+, proposto por Petri, Wangenheim e Borgatto (2019), permitindo uma avaliação mais sistemática e abrangente. O MEEGA+ permite medir aspectos como motivação, usabilidade e engajamento de forma padronizada, o que representa um alto grau de inovação quando comparado às abordagens utilizadas para avaliar jogos digitais educacionais com foco no ensino em cibersegurança. Essa abordagem não apenas permite avaliar o potencial do jogo, mas também oferece uma base metodológica robusta para futuras pesquisas na área de jogos digitais educacionais.

Com base nas lacunas identificadas na literatura e nos desafios observados nos trabalhos correlatos, evidencia-se a necessidade de uma abordagem metodológica que permita o desenvolvimento e a avaliação sistemática da proposta apresentada. Nesse contexto, são considerados aspectos relacionados à construção da ferramenta, à definição dos instrumentos de coleta de dados e aos procedimentos empregados para analisar sua aplicação no contexto educacional.

Capítulo 4

Método

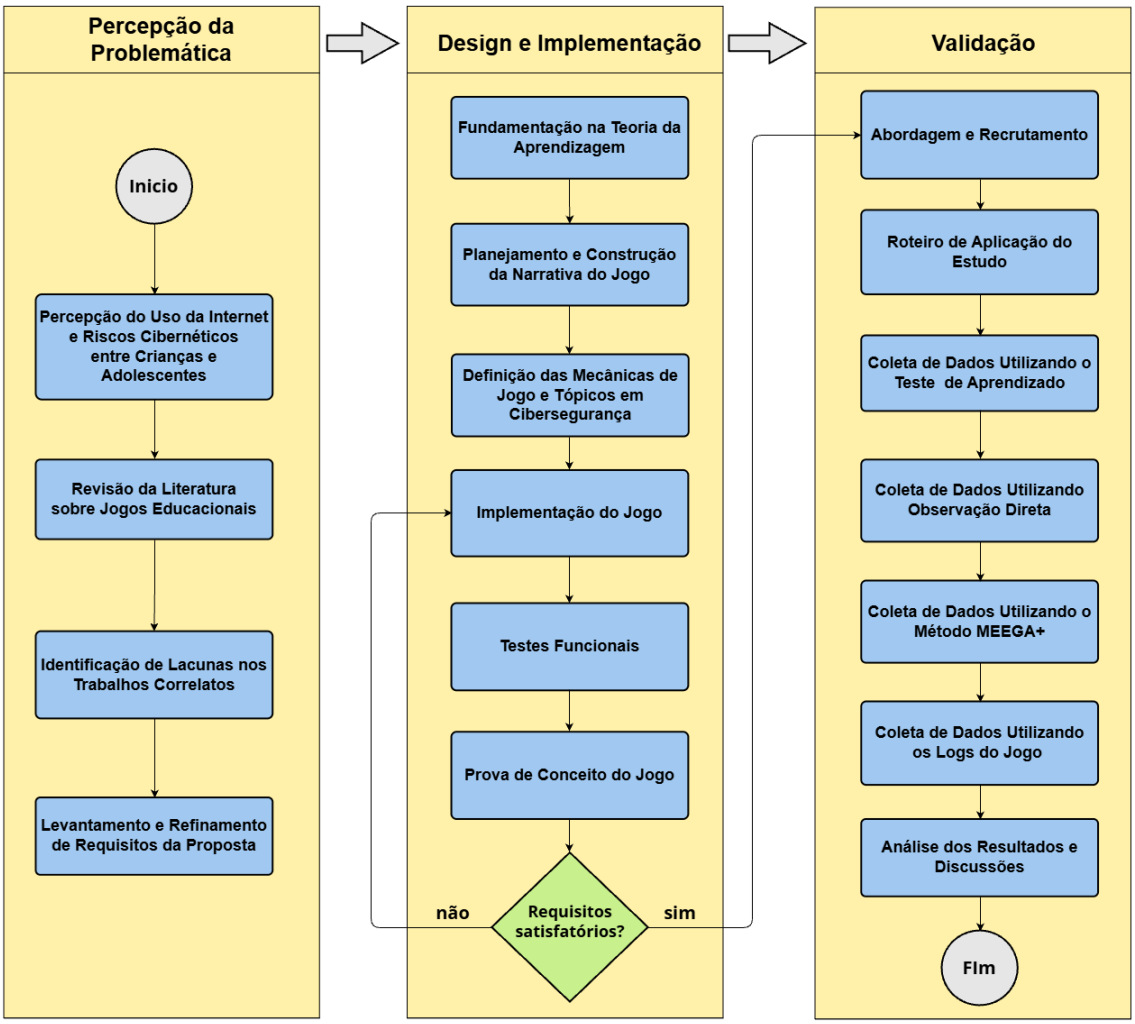
Esta pesquisa classifica-se, quanto à sua natureza, como aplicada, pois visa ao desenvolvimento de uma ferramenta educacional digital voltada ao aprendizado de segurança da informação para estudantes da educação básica, com fins práticos e utilitários no contexto pedagógico. Quanto aos objetivos, apresenta caráter exploratório, conforme a classificação proposta por Marconi e Lakatos (2004), por investigar uma temática ainda pouco explorada, buscando ampliar a compreensão do problema estudado e identificar aspectos relevantes do fenômeno analisado.

Trata-se de uma pesquisa aplicada, conforme a definição apresentada por Wazlawick (2009), de caráter tecnológico, uma vez que envolve o desenvolvimento de um artefato computacional, seguido de sua validação empírica junto ao público-alvo.

Considerando a natureza tecnológica desta pesquisa, sua condução foi estruturada com base em princípios da *Design Science Research* (DSR), conforme proposto por (PEFFERS et al., 2007). Essa abordagem serviu de referência para organizar a identificação do problema, a definição dos objetivos da solução, o desenvolvimento do artefato computacional e sua avaliação junto ao público-alvo. Nesse sentido, o estudo envolveu o desenvolvimento e o refinamento do jogo digital educacional Encrypta, seguidos de uma avaliação empírica de aspectos relacionados ao conhecimento em cibersegurança, à usabilidade e à experiência dos participantes.

O fluxograma apresentado na Figura 10 representa as etapas seguidas neste trabalho, acompanhado do detalhamento das atividades realizadas.

Figura 10 – Fluxograma de desenvolvimento da pesquisa.



Fonte: Elaboração Própria.

4.1 Percepção da Problemática

A etapa inicial de percepção da problemática é essencial para compreender o contexto no qual o projeto está inserido, abordando a questão da cibersegurança em relação ao público-alvo (crianças e adolescentes). Por meio dessa percepção inicial, foi possível identificar os desafios e os riscos enfrentados por esse público, além dos perigos aos quais estão constantemente expostos ao utilizar a internet. Com base nesse diagnóstico, foi realizada uma exploração da literatura atual para identificar ferramentas existentes que auxiliem no combate aos cibercrimes. A partir das abordagens selecionadas, iniciou-se a realização de uma análise crítica para identificar as lacunas deixadas por esses projetos, com o objetivo de preenchê-las no presente trabalho.

4.1.1 Percepção do Uso da Internet e Riscos Cibernéticos entre Crianças e Adolescentes

O desenvolvimento do projeto proposto partiu da análise dos desafios relacionados à segurança digital enfrentados por crianças e adolescentes, buscando compreender os riscos aos quais esse público está exposto no ambiente online. Para isso, foi realizado um estudo exploratório com o objetivo de investigar como crianças e adolescentes utilizam a internet e identificar comportamentos que possam aumentar sua exposição a riscos cibernéticos.

O estudo analisou aspectos como o uso de redes sociais, o tempo diário de acesso à internet, o compartilhamento de informações pessoais e outras práticas relacionadas à segurança digital. Os resultados permitiram caracterizar o perfil de uso da internet por esse público e identificar vulnerabilidades recorrentes, fornecendo subsídios para o planejamento das estratégias de conscientização adotadas no desenvolvimento da proposta.

4.1.2 Revisão da Literatura sobre Jogos Educacionais

A revisão da literatura desempenha um papel crucial no direcionamento da pesquisa, permitindo uma análise crítica dos projetos existentes que auxiliam na conscientização sobre cibersegurança. A partir desses projetos, foram identificadas as metodologias mais eficazes aplicadas atualmente e como elas podem ser adaptadas ou aprimoradas na proposta deste trabalho. A revisão também permitiu compreender as tendências atuais, as abordagens mais utilizadas e as limitações observadas nas iniciativas anteriores.

4.1.3 Identificação de Lacunas nos Trabalhos Correlatos

Com base nos projetos selecionados na revisão da literatura, foi possível identificar as lacunas deixadas por esses trabalhos, com o objetivo de concentrar a proposta deste projeto em áreas da cibersegurança que ainda não foram suficientemente exploradas ou que foram abordadas de forma superficial. Essas lacunas serviram como a base para o desenvolvimento do jogo educacional proposto, buscando preencher as deficiências existentes e oferecendo uma ferramenta de conscientização mais completa e eficaz. O objetivo é proporcionar uma experiência que, além de educativa, seja capaz de engajar os jovens na prática de boas medidas de segurança digital, ampliando a compreensão e a aplicação de conceitos de cibersegurança.

4.1.4 Levantamento e Refinamento de Requisitos da Proposta

Durante esta etapa, é fundamental estabelecer todos os requisitos necessários para a conclusão da implementação do jogo. Para isso, foram estabelecidos os objetivos do projeto proposto, detalhando os requisitos funcionais, não funcionais e pedagógicos da

aplicação. O objetivo principal desta etapa foi a identificação e organização das necessidades do projeto, a definição do seu escopo e a apresentação de uma base inicial, que serviu como ponto de partida para as próximas fases do desenvolvimento.

Na etapa de levantamento de requisitos, é fundamental apresentar os requisitos funcionais, não funcionais e pedagógicos do projeto, sendo estes:

- **Requisitos Funcionais**: Os requisitos funcionais são responsáveis por estabelecer as funcionalidades do *software*; em outras palavras, esses requisitos descrevem o que o sistema deve fazer, definindo suas entradas, saídas e exceções (ROLLWAGEN et al., 2020). Requisitos funcionais definem a forma como o *software* irá se comportar, ou seja, eles são fundamentais para estabelecer um direcionamento para a conclusão do projeto.

  Os requisitos funcionais foram levantados a partir da análise dos dados obtidos no estudo exploratório, que permitiu identificar as principais necessidades e vulnerabilidades relacionadas à segurança digital de crianças e adolescentes, e da análise de trabalhos correlatos, por meio da identificação das funcionalidades empregadas em jogos educacionais semelhantes. Com base nessas informações, foram definidas as funcionalidades que o jogo deveria oferecer para atender aos objetivos propostos pela pesquisa.

- **Requisitos Não-Funcionais**: Os requisitos não funcionais apresentam a forma como o sistema executará as funções estabelecidas pelos requisitos funcionais, como, por exemplo, as especificações de *hardware* necessárias para executar o *software*, questões relacionadas à segurança, confiabilidade, entre outros (ROLLWAGEN et al., 2020).

  Os requisitos não funcionais foram definidos considerando as características do público-alvo da pesquisa, composto por crianças e adolescentes, bem como as limitações do ambiente em que o jogo seria utilizado. Dessa forma, foram estabelecidos requisitos relacionados à usabilidade, acessibilidade, desempenho, confiabilidade e segurança, visando garantir uma experiência adequada aos usuários e ao contexto de aplicação da solução.

- **Requisitos Pedagógicos**: Por fim, os requisitos pedagógicos têm como objetivo garantir que o jogo seja eficaz como ferramenta educacional; em resumo, esses requisitos definem como este facilitará o aprendizado dos jogadores (SOUTO; SILVA, 2017).

  Os requisitos pedagógicos foram definidos com base na revisão da literatura sobre jogos educacionais, aprendizagem e conscientização em segurança digital, bem como nas competências e habilidades previstas pela BNCC relacionadas ao uso crítico, ético e seguro das tecnologias digitais. Esses requisitos orientaram decisões referentes ao conteúdo educacional, às mecânicas de aprendizagem, ao *feedback* fornecido

ao jogador e à organização das atividades propostas, buscando garantir que o jogo contribuísse para o alcance dos objetivos educacionais estabelecidos nesta pesquisa.

4.2 *Design* e Implementação

Durante a condução da pesquisa, ocorreu o desenvolvimento do jogo educacional. Nesta fase, aconteceu o planejamento e a construção da narrativa da proposta, a definição das mecânicas do jogo e a seleção dos tópicos de cibersegurança abordados por ele. Após a implementação, uma análise foi realizada para validar se os requisitos funcionais estabelecidos para a conclusão do projeto foram plenamente alcançados.

4.2.1 Fundamentação na Teoria da Aprendizagem

O desenvolvimento do Encrypta foi fundamentado em princípios de aprendizagem ativa, considerando que o conhecimento é construído a partir da interação do estudante com situações-problema contextualizadas. Dessa forma, além dos aspectos técnicos relacionados ao desenvolvimento do jogo, buscou-se incorporar fundamentos pedagógicos capazes de orientar a organização dos desafios, a progressão das fases e a forma como os conteúdos de cibersegurança são apresentados aos estudantes.

Sob a perspectiva construtivista proposta por Piaget (1976), a aprendizagem ocorre de maneira ativa, sendo resultado da interação do indivíduo com o meio. Nesse processo, novos conhecimentos são construídos por meio dos mecanismos de assimilação e acomodação, nos quais o estudante interpreta novas experiências, identifica limitações em seus conhecimentos prévios e reorganiza suas estruturas cognitivas. Considerando esses princípios, o jogo foi estruturado em fases com níveis progressivos de dificuldade, permitindo que os estudantes consolidassem conceitos já trabalhados antes de enfrentar novos desafios. Além disso, as atividades foram concebidas para incentivar a resolução de problemas, respeitando uma sequência crescente de complexidade compatível com o desenvolvimento cognitivo esperado para o público-alvo.

Complementando essa abordagem, a perspectiva construcionista de Papert (1980) destaca que a aprendizagem é potencializada quando o estudante assume um papel ativo na construção do conhecimento, aprendendo por meio da experimentação, da resolução de problemas e da reflexão sobre suas próprias ações. Com base nesses princípios, o Encrypta foi desenvolvido de modo que os estudantes interajam continuamente com os desafios apresentados, recebendo *feedback* imediato sobre suas decisões. Dessa forma, o erro é compreendido como parte natural do processo de aprendizagem, permitindo que novas estratégias sejam testadas por meio da repetição das fases e da experimentação contínua, favorecendo a consolidação gradual dos conceitos de cibersegurança.

Por fim, sob a perspectiva socioconstrutivista de Vygotsky (1991), a aprendizagem é favorecida pela interação social e pela mediação realizada por indivíduos mais experientes,

conceito representado pela Zona de Desenvolvimento Proximal. Nesse contexto, embora o jogo possa ser utilizado individualmente, sua aplicação foi concebida para ocorrer preferencialmente em ambiente escolar, permitindo que professores atuem como mediadores do processo de aprendizagem, esclarecendo dúvidas, contextualizando os desafios e estimulando discussões entre os estudantes. Além disso, o compartilhamento de experiências e a colaboração entre os participantes são incentivados durante a utilização da ferramenta, contribuindo para a construção coletiva do conhecimento.

Dessa forma, a estratégia pedagógica adotada no desenvolvimento do Encrypta integra princípios construtivistas, construcionistas e socioconstrutivistas, buscando promover uma aprendizagem ativa por meio da resolução de problemas, da experimentação, da reflexão sobre as próprias ações e da interação entre estudantes, professor e tecnologia. Esses princípios orientaram a definição das mecânicas do jogo, a progressão dos desafios, o fornecimento de *feedback* imediato, a contextualização da narrativa e a associação dos conteúdos de cibersegurança a situações próximas da realidade vivenciada pelos estudantes.

4.2.2 Planejamento e Construção da Narrativa do Jogo

Durante a etapa de construção e planejamento da narrativa, foram definidos os artefatos responsáveis por compor o enredo do jogo. Esse processo envolveu a elaboração da história central, a caracterização dos personagens e a definição dos eventos que conduziriam o jogador ao longo da experiência, buscando manter uma sequência lógica entre os desafios apresentados.

Além dos aspectos narrativos, procurou-se integrar os conceitos de segurança digital às situações vivenciadas pelos personagens. Dessa forma, temas como criação de senhas seguras, golpes de *phishing* e boas práticas de navegação foram incorporados ao contexto da história, permitindo que os conteúdos educacionais fossem apresentados de maneira contextualizada e relacionados a situações semelhantes às enfrentadas pelo público-alvo.

A construção da narrativa teve como objetivo favorecer o engajamento dos jogadores e fornecer um contexto para as atividades propostas. Assim, os desafios e diálogos foram desenvolvidos para que os conceitos abordados estivessem alinhados aos objetivos educacionais definidos para a ferramenta.

4.2.3 Definição das Mecânicas de Jogo e Tópicos em Cibersegurança

Durante esta etapa do desenvolvimento, foram definidas as mecânicas do jogo e selecionados os tópicos de cibersegurança a serem abordados, tomando como referência as competências e habilidades previstas na BNCC para o Ensino Básico.

A integração dos conceitos ocorreu por meio da contextualização dos temas de segurança digital em eventos da história e em atividades interativas do jogo. Dessa forma, os jogadores eram incentivados a identificar riscos, tomar decisões diante de situações simuladas e receber *feedback* sobre as consequências de suas escolhas, favorecendo a reflexão sobre boas práticas de segurança digital.

O alinhamento com os objetivos pedagógicos foi realizado ao garantir que cada fase do jogo contemplasse conteúdos e desafios compatíveis com as competências educacionais previamente definidas, permitindo que os elementos narrativos, as mecânicas e as atividades contribuíssem conjuntamente para o processo de aprendizagem.

4.2.4 Implementação do Jogo

No estágio de implementação, ocorreu o desenvolvimento do projeto utilizando os requisitos e as ferramentas estabelecidas nas etapas anteriores. Nesta fase do projeto, foram implementados os *scripts* referentes ao seu funcionamento, bem como toda a elaboração da lógica de programação necessária para realizar o desenvolvimento. Além disso, foram realizadas as construções de fases e cenários utilizando as tecnologias definidas. Para a gestão das tarefas, utilizou-se a ferramenta Trello[1] com a metodologia Kanban, que consiste em um sistema visual de gestão de fluxo de trabalho, o que permitiu o acompanhamento das *sprints* (ciclos de desenvolvimento de curta duração).

O processo de construção do artefato seguiu uma abordagem de desenvolvimento iterativo, mantendo um histórico de versões executáveis na plataforma de jogos independentes Itch.io[2]. Esse método permitiu o acompanhamento da evolução do projeto e a disponibilização frequente de *builds* prontas para validação e testes. Por fim, o código-fonte do projeto foi consolidado em um repositório público no GitHub [3].

4.2.5 Testes Funcionais

Nesta etapa, foi verificado se o jogo desenvolvido atendia aos requisitos técnicos e funcionais definidos nas etapas anteriores, assegurando a implementação adequada das funcionalidades planejadas. Para isso, foram executados testes exploratórios conduzidos pelo autor, nos quais cada funcionalidade do jogo foi utilizada em diferentes cenários de interação, simulando o comportamento esperado do usuário.

Durante os testes, foram avaliados aspectos como a navegação entre as fases, o funcionamento das mecânicas do jogo, o sistema de colisões, o controle de vidas, a exibição dos *feedbacks* ao jogador e o correto acionamento dos eventos previstos na narrativa. Sempre que um comportamento diferente do esperado era identificado, eram realizados ajustes no

[1] https://trello.com/
[2] https://itch.io/
[3] Disponível em: https://github.com/jeanlucamtp12/Encrypta/

código e uma nova rodada de testes era executada para verificar se a inconsistência havia sido corrigida.

Os testes foram concluídos quando todas as funcionalidades previstas operavam conforme os requisitos estabelecidos, permitindo que o jogo fosse encaminhado para a etapa de validação com usuários.

4.2.6 Prova de Conceito do Jogo

Após a aprovação nos testes funcionais, foi realizada uma *Proof of Concept* (PoC) do jogo, com o objetivo de coletar *feedbacks* sobre aspectos de usabilidade e da experiência do jogador.

A PoC teve como objetivo coletar sugestões dos usuários em relação à viabilidade de prosseguimento do desenvolvimento do projeto. A partir dos dados obtidos, foram identificadas oportunidades de melhoria que orientaram a refatoração da versão inicial, permitindo que o jogo prosseguisse para a etapa de validação.

4.3 Validação

Na etapa de validação, foi conduzido o estudo empírico com o público-alvo, com o objetivo de coletar dados suficientes para uma análise aprofundada sobre como a proposta contribui para o ganho de conhecimento em cibersegurança. Com base nos resultados obtidos, foi possível avaliar se o projeto atingiu os objetivos propostos e se obteve resultados satisfatórios para sua finalização e alcance das metas estabelecidas.

4.3.1 Abordagem e Recrutamento

Para a realização do estudo com a comunidade escolar, foi necessário realizar uma abordagem inicial que considerasse os aspectos éticos, logísticos e metodológicos envolvidos no recrutamento dos participantes. Esta seção apresenta a população definida para a participação nesta pesquisa, as etapas iniciais, que incluem a visita e mapeamento da instituição selecionada para participar do projeto, os aspectos éticos adotados para sua conclusão e a apresentação da proposta aos pais e responsáveis pelos participantes.

- ❑ **Visita Inicial à Instituição**: Foi realizada uma visita ao Colégio de Aplicação da Universidade Federal de Uberlândia (CAp/UFU) com o objetivo de apresentar brevemente o projeto à diretora da instituição e esclarecer os objetivos da pesquisa. Na ocasião, foram definidos aspectos essenciais para o desenvolvimento do estudo, como o número aproximado de estudantes participantes, as turmas disponíveis e outras condições logísticas e éticas para a aplicação dos testes.

- **Apresentação do Projeto aos Responsáveis pelos Estudantes**: Com o objetivo de esclarecer possíveis dúvidas acerca da pesquisa e apresentar os detalhes do projeto, foi solicitada pela escola a elaboração de um material de divulgação, composto por um *card* informativo e um texto explicativo. Esses materiais foram enviados às famílias por meio do aplicativo de mensagens instantâneas utilizado pela instituição (WhatsApp), abordando os objetivos do estudo, os procedimentos a serem adotados durante a aplicação dos testes e as medidas éticas envolvidas.

  Além disso, foram encaminhados aos pais e responsáveis o Termo de Consentimento Livre e Esclarecido (TCLE) (Apêndice D), para a autorização formal da participação dos estudantes na pesquisa, bem como o Termo de Assentimento (TA) (Apêndice C), assinado pelos próprios estudantes, garantindo sua participação voluntária. Esses documentos também tiveram como objetivo assegurar aos responsáveis que a pesquisa seria conduzida de forma ética e com garantia de anonimato dos participantes. Visando garantir a participação adequada dos estudantes, o CAp/UFU prestou apoio logístico no envio e na coleta dos termos.

- **Caracterização da Instituição de Ensino**: O (CAp/UFU), instituição pública vinculada à Universidade Federal de Uberlândia (UFU). Localizada no Campus Educação Física (FAEFI) em Uberlândia - MG, a unidade foi selecionada por sua natureza de escola de aplicação, o que favorece o desenvolvimento de investigações científicas e a implementação de metodologias ativas no ensino básico.

  A instituição atende estudantes desde a Educação Infantil até o Ensino Fundamental, operando em regime de tempo integral. Para a realização da pesquisa, foram selecionadas turmas do Ensino Fundamental, abrangendo 12 turmas do 4º ao 7º ano, com média de 20 estudantes por turma, totalizando aproximadamente 240 estudantes, com idades entre 8 e 14 anos. A amostra incluiu as turmas A, B e C de cada ano, todas pertencentes ao turno matutino.

  Para a execução da intervenção, a instituição de ensino disponibilizou as aulas de Matemática, com a possibilidade de utilização do laboratório de informática durante o horário das aulas para a aplicação do projeto em cada uma das turmas participantes. Dessa forma, o cronograma de aplicação foi estruturado de modo a respeitar a grade horária escolar, conforme detalhado na Tabela 4.

Tabela 4 – Cronograma de intervenção e coleta de dados.

Horário	**23/03/26 (Seg)**	**24/03/26 (Ter)**	**25/03/26 (Qua)**	**26/03/26 (Qui)**	**27/03/26 (Sex)**	**30/03/26 (Seg)**
07h30–08h20	—	4º B		7º C*	6º B	4º C
08h20–09h10	7º B	4º B	5º B	7º C*	6º B	4º C
09h10–09h30	7º B	—	—	—	—	—
09h30–10h20	—	4º A	5º B	—	—	5º C
10h20–11h10	7º A	4º A	5º A	6º C	6º A	5º C
11h10–12h00	7º A	—	5º A	6º C	6º A	—

Fonte: Elaboração própria.

Com base na Tabela 4, a turma do 7º C, inicialmente prevista no roteiro de aplicação do estudo e no cronograma elaborado, foi excluída do projeto, uma vez que nenhum dos estudantes apresentou os termos de consentimento e assentimento necessários para assegurar sua participação. Essa medida visa garantir a adequação ética da pesquisa.

- **Infraestrutura Tecnológica e Ambiente de Aplicação**: Para a realização do projeto, a escola disponibilizou um laboratório de informática, utilizado para a execução das atividades. O laboratório possui 14 computadores e 6 notebooks com sistema operacional Windows disponíveis para uso, sendo possível utilizar todos os equipamentos. Alguns dos dispositivos apresentaram pequenos problemas técnicos em determinados momentos da atividade; no entanto, isso não impactou o andamento da pesquisa, considerando o número inferior de estudantes participantes.

  Para a realização do projeto, e devido à ausência de acesso à internet em alguns dos computadores, o jogo foi instalado por meio de sua versão *desktop*, a qual não exige conexão com a internet, sendo necessária sua instalação em cada uma das máquinas. O laboratório dispunha de cadeiras individuais para cada um dos estudantes, que puderam escolher livremente seus lugares, permanecendo lado a lado com os demais participantes, o que possibilitou a interação entre eles.

  Além disso, durante toda a atividade, o professor responsável pela aula de Matemática no respectivo turno permaneceu disponível no laboratório para auxiliar em qualquer situação que pudesse ocorrer.

- **Aspectos Éticos e Critérios para Participação**

  Como a proposta metodológica envolve a coleta de dados com participantes humanos, houve a submissão e aprovação do projeto pelo Comitê de Ética em Pesquisa

com Seres Humanos (CEP) da UFU[4], em conformidade com as diretrizes éticas vigentes. Foram definidos os seguintes critérios para participação no estudo:

Critérios de Inclusão

Para participar dos testes deste projeto, o estudante precisou atender aos seguintes critérios de inclusão:

- Estar regularmente matriculado em turmas do 4º ao 7º ano do Ensino Fundamental do CAp/UFU;
- Apresentar autorização formal dos pais ou responsáveis legais por meio do TCLE;
- Apresentar concordância em participar da pesquisa por meio do TA.

Critérios de Exclusão

Foi excluído da participação no estudo o estudante que se enquadrou em um ou mais dos seguintes critérios:

- Não apresentar o TCLE devidamente assinado pelos pais ou responsáveis legais;
- Não apresentar o TA, devidamente assinado pelo próprio estudante;
- Não estiver regularmente matriculado em turmas do 4º ao 7º ano do Ensino Fundamental do CAp/UFU;
- Estiver ausente da instituição de ensino no(s) dia(s) previsto(s) para a aplicação dos testes;
- Optar por desistir da participação no decorrer das atividades ou não completar integralmente as etapas previstas do estudo.

❑ **População do Estudo**: A aplicação dos testes foi realizada ao longo de oito dias, compreendendo uma semana completa e o início da semana subsequente, contemplando turmas do 4º ao 7º ano do Ensino Fundamental do CAp/UFU. No total, este universo é composto por 240 estudantes, com idades entre 8 e 14 anos.

A amostra para a realização dos testes foi composta por 110 estudantes, dimensionada por meio da fórmula para populações finitas sugerida por Gil (1995), considerando-se uma margem de erro de 6% e um nível de confiança de 95%.

[4] Certificado de Apresentação para Apreciação Ética (CAAE): nº 91510925.4.0000.5152

4.3.2 Roteiro de Aplicação do Estudo

O roteiro de aplicação do estudo apresentado nesta seção é composto por quatro etapas distintas, cada uma com objetivos específicos. A primeira etapa consiste na apresentação do projeto aos estudantes envolvidos na pesquisa; já a segunda envolve a aplicação do questionário de pré-teste para avaliação do conhecimento prévio dos estudantes; a terceira etapa contempla a utilização do jogo educacional e a coleta de *logs* e observação direta, seguida da última etapa, na qual os questionários de pós-teste e MEEGA+ foram aplicados. A seguir, apresenta-se o roteiro detalhado das etapas que conduziram a pesquisa:

- **Etapa 1 - Apresentação do Projeto**: Em um primeiro momento, os estudantes foram apresentados aos pesquisadores envolvidos no projeto, bem como aos objetivos gerais do estudo, sendo também contextualizados sobre a proposta.

  A apresentação teve duração aproximada de cinco minutos, período no qual foram fornecidas orientações gerais sobre as atividades a serem realizadas, conforme as etapas seguintes, com o intuito de esclarecer as principais dúvidas e promover um ambiente acolhedor e propício à participação dos estudantes.

- **Etapa 2 - Etapa de Pré-teste**: Logo após a apresentação do projeto, os estudantes foram conduzidos ao laboratório de informática da instituição e convidados a responder ao questionário de pré-teste. Esse questionário, composto por 15 questões objetivas relacionadas a conceitos básicos de cibersegurança (Apêndice A), teve como finalidade identificar o nível de conhecimento prévio dos participantes sobre o tema.

  A aplicação teve duração estimada entre 10 e 15 minutos por turma. Foram disponibilizados materiais, como questionários impressos e canetas, para todos os estudantes envolvidos.

- **Etapa 3 - Sessão de Utilização do Jogo**: Após a finalização do questionário de pré-teste, os estudantes tiveram aproximadamente 60 minutos para interagir com o jogo Encrypta. A atividade foi realizada de forma individual, permitindo que cada participante explorasse o jogo em seu próprio ritmo e tomasse decisões de maneira autônoma ao longo das fases propostas.

- **Etapa 3.1 - Protocolo de Observação Direta**: Em paralelo à execução da atividade, foi realizada a observação direta do comportamento e das reações dos participantes durante a interação com o jogo. Os registros dessas observações foram anotados em um diário de campo, contemplando aspectos relacionados às necessidades, dificuldades e desempenho dos estudantes ao longo de cada dia do estudo.

- ❑ **Etapa 3.2 - Registro Automatizado via *Logs* do Sistema**: Durante a execução do jogo pelos estudantes, o *software* realizou o registro automatizado de *logs* contendo informações sobre o desempenho dos participantes, incluindo erros e acertos ao longo das fases, bem como o tempo de utilização da aplicação.

- ❑ **Etapa 4 - Procedimentos de Pós-Intervenção**: Após a conclusão do jogo, os estudantes foram convidados a finalizar a atividade por meio do preenchimento do questionário de pós-teste (mesmo questionário do pré-teste, conforme apêndice A) e do questionário MEEGA+ (Apêndice B).

- ❑ **Etapa 4.1 - Etapa de Pós-teste**: Os estudantes responderam novamente ao questionário de 15 questões sobre cibersegurança, com o objetivo de avaliar possíveis avanços no conhecimento em comparação com o pré-teste aplicado anteriormente. A aplicação teve duração estimada de 10 minutos, utilizando os mesmos materiais da etapa de pré-teste (questionários e canetas).

- ❑ **Etapa 4.2 - Aplicação do Questionário MEEGA+**: Por fim, os participantes preencheram o questionário MEEGA+, com duração estimada de 10 minutos, que teve como objetivo avaliar a experiência do usuário em relação à usabilidade e experiência do jogador. Assim como nas etapas anteriores, foram fornecidos questionários impressos e canetas.

- ❑ **Duração Total do Roteiro de Aplicação do Estudo**: A duração total do estudo foi estimada em aproximadamente 100 minutos por turma e, de modo geral, foi executada conforme o planejado, sem a ocorrência de problemas técnicos, como falhas de conectividade ou dificuldades na configuração dos equipamentos.

  Entretanto, em três das 11 turmas participantes, houve a disponibilidade de apenas um horário no laboratório de informática da instituição, limitando a atividade a cerca de 50 minutos. Nesses casos, os estudantes realizaram o pré-teste, participaram da apresentação do projeto e interagiram com o jogo nesse período reduzido, sendo necessário concluir os questionários de pós-teste e MEEGA+ em sala de aula.

A Tabela 5 apresenta um resumo das etapas que compõem o roteiro de aplicação do estudo, incluindo os tempos estimados para cada uma delas, os recursos necessários e o tempo total previsto para a conclusão delas.

Tabela 5 – Roteiro de aplicação do estudo.

Etapa	**Tempo Estimado**	**Recursos Necessários**
Apresentação do Projeto	≈ 5 minutos	—
Pré-teste	≈ 15 minutos	Questionário impresso, caneta
Sessão de utilização do jogo	≈ 60 minutos	Computadores (1 por estudante)
Pós-teste	≈ 10 minutos	Questionário impresso, caneta
Questionário MEEGA+	≈ 10 minutos	Questionário impresso, caneta
Tempo Total Estimado	**≈ 100 minutos**	

Fonte: Elaboração própria.

4.3.3 Coleta de Dados Utilizando o Teste de Conhecimento

O teste de conhecimento, no formato de questões de múltipla-escolha (*quiz*), correspondeu ao mesmo instrumento utilizado na sexta fase do jogo, que consiste em um *quiz* com 15 questões relacionadas aos tópicos abordados pela aplicação, tais como: uso de senhas fortes, detecção de e-mails de *phishing*, identificação de pastas potencialmente maliciosas, reconhecimento de sites fraudulentos e a importância da realização de *backups* regulares de dados.

Com o objetivo de facilitar a coleta e a padronização dos dados, esse *quiz* foi adaptado para o formato de questionário impresso. Dessa forma, durante a utilização do jogo, a sexta fase foi bloqueada para todos os participantes, uma vez que o conjunto de questões já havia sido respondido externamente, evitando a reaplicação do mesmo instrumento.

A aplicação desse teste ocorreu em duas etapas. Inicialmente, o questionário foi aplicado como pré-teste, antes de os participantes entrarem em contato com a aplicação. Após a utilização da ferramenta, foi realizado o pós-teste, utilizando exatamente o mesmo conjunto de questões aplicado no pré-teste. A adoção do mesmo instrumento teve como objetivo comparar o desempenho dos participantes antes e após a intervenção, permitindo verificar possíveis ganhos de conhecimento em cibersegurança decorrentes da utilização do jogo.

Os estudantes foram orientados a responder aos questionários de forma individual, sem auxílio externo ou dos colegas, sendo também instruídos a circularem ou indicarem,

por meio de sinais de interrogação, palavras ou termos que não conheciam.

4.3.4 Coleta de Dados Utilizando Observação Direta

Durante a execução da pesquisa, foi aplicada a metodologia de observação direta, que consiste em ver, ouvir e examinar o objeto de estudo com o objetivo de coletar dados de forma reflexiva e descritiva. Tal abordagem exige que o pesquisador mantenha contato direto com o objeto investigado, podendo variar entre uma imersão mais intensa e um maior distanciamento (ANA; LEMOS, 2018).

No contexto deste projeto, buscou-se adotar uma postura de mínima interferência durante a atividade. Aos estudantes, foi sugerido um percurso inicial no jogo, iniciando pelo primeiro personagem e seguindo até o último, sem, contudo, impor essa sequência, permitindo que explorassem livremente a aplicação e conduzissem sua própria experiência.

Durante a observação, foram registrados em diário de campo aspectos relacionados ao comportamento dos participantes, incluindo dúvidas recorrentes, solicitações de ajuda, dificuldades na compreensão das mecânicas do jogo, reações aos *feedbacks* apresentados, estratégias adotadas para solucionar os desafios e demonstrações de interesse ou frustração ao longo da atividade. Também foram registradas eventuais falhas técnicas observadas durante a execução da ferramenta.

As intervenções ocorreram apenas em momentos pontuais, quando solicitadas pelos próprios participantes. Essa postura teve como objetivo preservar a espontaneidade da interação com o jogo, permitindo registrar o comportamento dos estudantes e avaliar seu nível de engajamento com os elementos lúdicos da ferramenta, como personagens, narrativa, mecânicas e elementos visuais.

As observações registradas possibilitaram identificar momentos em que os estudantes apresentaram maiores facilidades e dificuldades durante a utilização da aplicação. Posteriormente, esses registros foram analisados em conjunto com os dados obtidos por meio dos questionários, dos testes de conhecimento e dos arquivos de *logs*, contribuindo para a análise dos dados e para uma compreensão mais abrangente da interação dos participantes com a ferramenta e com os conteúdos de cibersegurança abordados.

4.3.5 Coleta de Dados Utilizando o Método MEEGA+

Após a conclusão dos testes de conhecimento, os participantes foram convidados a responder ao questionário MEEGA+, amplamente utilizado para avaliar a percepção sobre jogos educacionais. Este método analisa a aplicabilidade e o potencial pedagógico da ferramenta sob a ótica da usabilidade e da experiência do jogador (PETRI; WANGENHEIM; BORGATTO, 2019). Tais dimensões são estruturadas a partir dos seguintes pilares:

Usabilidade, mensurada em cinco subdimensões:

- ❑ **Estética:** Grau de atração visual da interface ou componentes do jogo.
- ❑ **Aprendizibilidade:** Facilidade com que novos jogadores aprendem as regras e mecânicas.
- ❑ **Operabilidade:** Clareza e simplicidade na execução das ações previstas pelo jogo.
- ❑ **Acessibilidade:** Adequação do jogo a diferentes perfis de jogadores (legibilidade de textos, distinção de cores etc.).
- ❑ **Proteção contra Erros:** Mecanismos que evitam ou permitem corrigir falhas do usuário durante o jogo.

Experiência do Jogador, composta por oito subdimensões:

- ❑ **Confiança:** Percepção de competência e sensação de progresso ao longo do jogo.
- ❑ **Desafio:** Oferta de obstáculos e variação de dificuldades para manter o interesse.
- ❑ **Satisfação:** Grau de prazer e realização ao completar tarefas ou objetivos.
- ❑ **Interação Social:** Potencial para cooperação, competição e trabalho em equipe entre os participantes.
- ❑ **Diversão:** Capacidade do jogo de envolver emocionalmente e promover entretenimento.
- ❑ **Atenção Focada:** Nível de concentração e imersão, incluindo a perda da noção de tempo.
- ❑ **Relevância:** Pertinência dos conteúdos e cenários em relação aos objetivos educacionais e ao contexto do tema.
- ❑ **Aprendizagem Percebida:** Avaliação subjetiva do quanto o jogo contribuiu para o aprendizado em comparação a outras atividades.

4.3.6 Coleta de Dados Utilizando os *Logs* do Jogo

De forma complementar aos questionários e observação direta, foram coletados os *logs* gerados pelos usuários durante as atividades. Os registros associados às fases do jogo fornecerão informações relevantes, como o tempo despendido por cada jogador em cada fase, bem como a ocorrência de repetições ou abandonos delas.

Adicionalmente, foram coletados dados específicos de cada fase. Entre eles, destacam-se: a quantidade de senhas seguras e inseguras criadas pelos participantes; o número

de pastas inofensivas e maliciosas coletadas; a identificação de e-mails de *phishing*, bem como a classificação incorreta de e-mails legítimos como maliciosos; e, ainda, a detecção de elementos inofensivos ou maliciosos na fase relacionada a websites, conforme apresentado na Tabela 6.

Tabela 6 – *Logs* coletados em cada fase do jogo.

Fase	***Logs* específicos**	***Logs* gerais**
Fase 1 (Senhas)	Senhas seguras criadas Senhas inseguras criadas	Tempo gasto Abandono da fase Conclusão da fase
Fase 2 (E-mails)	Detecção correta de *phishing* Detecção incorreta de *phishing*	Tempo gasto Abandono da fase Conclusão da fase
Fase 3 (Arquivos)	Arquivos maliciosos coletados Arquivos inofensivos coletados	Tempo gasto Abandono da fase Conclusão da fase
Fase 4 (Sites)	Pontos maliciosos clicados Pontos inofensivos clicados	Tempo gasto Abandono da fase Conclusão da fase
Fase 5 (*Backup*)	—	Tempo gasto Abandono da fase Conclusão da fase

Fonte: Elaboração própria.

4.3.7 Análise Estatística

Para avaliar as diferenças antes e depois da aplicação do jogo, a escolha por testes não paramétricos foi motivada pela ausência de normalidade na distribuição dos dados. Embora as variáveis de desempenho individual sejam dicotômicas (acerto ou erro), a análise estatística considerou os escores totais obtidos nos momentos de pré e pós-teste.

A normalidade dos dados foi avaliada por meio do teste de Shapiro-Wilk (SHAPIRO; WILK, 1965). Considerando que valores de $p < 0{,}05$ indicam violação da hipótese de normalidade, esse teste foi utilizado para verificar se os dados seguiam uma distribuição normal. A homogeneidade das variâncias (homocedasticidade) foi avaliada por meio do teste de Levene, no qual valores de $p > 0{,}05$ indicam variâncias homogêneas (LEVENE, 1960). Com base nos resultados desses testes, definiu-se a abordagem estatística mais adequada para as análises subsequentes. Para verificar as diferenças significativas entre os resultados obtidos antes e após a aplicação do jogo, utilizou-se o teste de Wilcoxon (WILCOXON, 1945).

Complementarmente ao teste de Wilcoxon, para mensurar a magnitude da diferença observada, foi utilizado o tamanho de efeito (r). A interpretação dos valores seguiu as

diretrizes propostas por Cohen (1988), sendo: valores próximos de 0,10 indicam efeito pequeno (fraco), valores em torno de 0,30 indicam efeito médio (moderado) e valores acima de 0,50 indicam efeito grande (forte).

A métrica de Ganho de Hake (g), proposta por Hakea (1998) também foi utilizada para verificar o ganho de conhecimento. Este método é amplamente aplicado na avaliação de intervenções educacionais, baseando-se na comparação do desempenho dos participantes entre o pré e o pós-teste. O cálculo permite quantificar a eficácia da ferramenta no processo de ensino-aprendizagem através da seguinte expressão:

$$g = \frac{\%Pós - \%Pré}{100\% - \%Pré} \tag{1}$$

Onde:

- g é o ganho normalizado;
- $\%Pós$ é a média de acertos no pós-teste;
- $\%Pré$ é a média de acertos no pré-teste.

O teste de McNemar também foi utilizado para realizar uma análise individual de cada uma das 15 questões do teste de conhecimento (MCNEMAR, 1947). Valores de $p < 0{,}05$ indicam evidências suficientes para rejeitar a hipótese nula e indicar mudança estatisticamente significativa nas proporções entre os dois momentos analisados.

Além disso, foram utilizadas medidas descritivas, como média e desvio padrão, para complementar a análise dos resultados relacionados à etapa de ganho de conhecimento (BUSSAB; MORETTIN, 2010).

Nas análises de usabilidade e experiência do jogador, também foram empregados testes não paramétricos. Inicialmente, a normalidade dos dados foi avaliada por meio do teste de Shapiro-Wilk. Adicionalmente, o teste de Levene foi aplicado para verificar a homogeneidade das variâncias. Com base nos resultados desses testes, definiu-se a abordagem estatística mais adequada para as análises subsequentes. A análise das correlações foi realizada por meio do coeficiente de correlação de postos de Spearman (SPEARMAN, 1961).

Complementando a análise, foi aplicada regressão linear múltipla com o objetivo de verificar como a combinação de diferentes esferas do modelo influenciou a variável dependente Aprendizagem Percebida (HAIR et al., 2009). Quando identificada heterocedasticidade, os modelos foram estimados com erros-padrão robustos por meio do estimador HC3, visando reduzir possíveis vieses nas inferências estatísticas.

O Coeficiente de Variação (CV), apresentado por Bussab e Morettin (2010), foi utilizado para verificar a homogeneidade das respostas e o grau de consenso entre os participantes. Diferente do desvio padrão absoluto, o CV permite uma análise da dispersão relativa à média, facilitando a comparação entre as diferentes dimensões do MEEGA+.

Para a interpretação dos resultados, obtém-se a classificação de que valores de $CV \leq 15\%$ indicam baixa dispersão (alto consenso), $15\% < CV \leq 30\%$ indicam dispersão média e $CV > 30\%$ representam heterogeneidade nas respostas, conforme a seguinte expressão:

$$CV = \frac{S}{\bar{x}} \times 100\% \tag{2}$$

Onde:

- CV é o Coeficiente de Variação;
- S representa o Desvio Padrão amostral;
- $\bar{x}$ corresponde à Média aritmética da amostra.

Por fim, a normalidade dos dados provenientes dos *logs* do jogo foi avaliada para subsidiar a escolha dos métodos estatísticos mais adequados. Com base nessa avaliação, a análise dos *logs* foi conduzida por meio da correlação de Spearman. O objetivo foi realizar o cruzamento entre as diversas métricas geradas pelas fases do jogo, bem como relacioná-las aos resultados obtidos nas etapas anteriores (pré e pós-teste e MEEGA+).

Por meio do teste de Levene, foi avaliada a homogeneidade das variâncias entre as métricas de tempo, erros, acertos, abandonos e taxa de conclusão, com o objetivo de verificar a variabilidade entre essas medidas. Essa análise permitiu caracterizar a consistência das métricas e subsidiar a interpretação do comportamento dos jogadores ao longo das fases do jogo.

4.3.8 Análise dos Resultados e Discussões

Nesta etapa, com base nos resultados dos testes realizados, foram analisados aspectos de usabilidade, experiência do jogador, observação direta, *logs* e aprendizado. A avaliação de usabilidade abordou fatores como facilidade de uso, intuitividade, consistência do *design* e clareza na apresentação das informações. O estudo da experiência do jogador enfocou aspectos de motivação e engajamento durante a interação com a aplicação. A análise da observação direta foi utilizada como complemento aos dados quantitativos obtidos, enquanto os *logs* da aplicação serviram para verificar o desempenho e o comportamento dos estudantes durante o jogo. Por fim, a análise do aprendizado considerou o desempenho dos estudantes na resolução de questões sobre cibersegurança, comparando os resultados obtidos antes e após a utilização da ferramenta. A partir dessa análise, foi possível validar se a proposta atendeu satisfatoriamente aos objetivos educacionais apresentados, empregando métricas estatísticas para a interpretação dos resultados.

Capítulo 5

Design e Implementação do Jogo Encrypta

Este capítulo apresenta a história criada para o jogo, os tópicos de cibersegurança abordados pela aplicação, além de descrever as ferramentas utilizadas no processo de desenvolvimento do *software*.

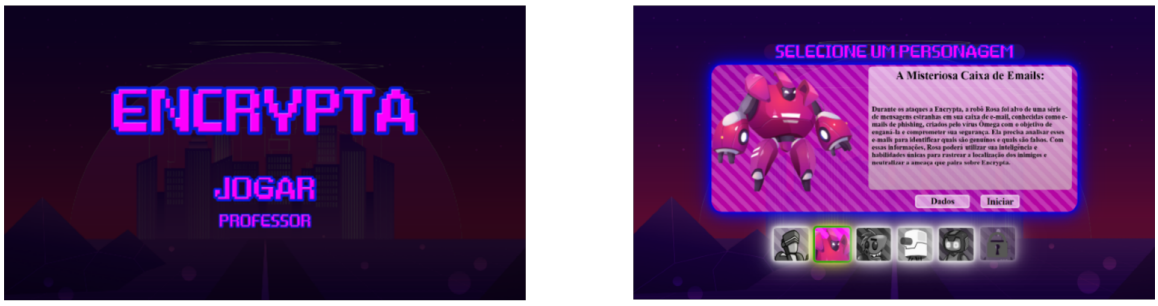
5.1 História do Jogo

A seguir, apresenta-se o esboço da narrativa concebida para o jogo, que serviu como fundamento para o desenvolvimento do enredo e da definição das interações dos jogadores com a ferramenta:

> *"Encrypta: A missão da Liga dos Robôs" é um jogo digital educacional voltado para adolescentes do ensino básico, desenvolvido com o propósito de conscientizá-los sobre os perigos do ambiente virtual. Ao longo da narrativa, os jogadores conhecem os seis integrantes da Liga dos Robôs, uma equipe de heróis responsável por manter a ordem na futurista cidade de Encrypta. O jogo é estruturado em seis fases temáticas, compostas por minijogos, quizzes e desafios que exploram diferentes aspectos da cibersegurança.*

Ao iniciar, os participantes descobrem que a cidade foi atacada por um poderoso vírus denominado Ômega. Diante dessa ameaça, a Liga dos Robôs se une para restaurar a paz e combater os danos causados. Cada personagem possui uma história própria, representada em uma fase específica, na qual os jogadores devem auxiliá-los a enfrentar e combater o vírus maligno. A Figura 11 apresenta a tela inicial elaborada para o jogo, bem como a tela de seleção de personagens.

Figura 11 – Capturas de tela: a) Tela inicial do jogo; b) Seleção de personagens.

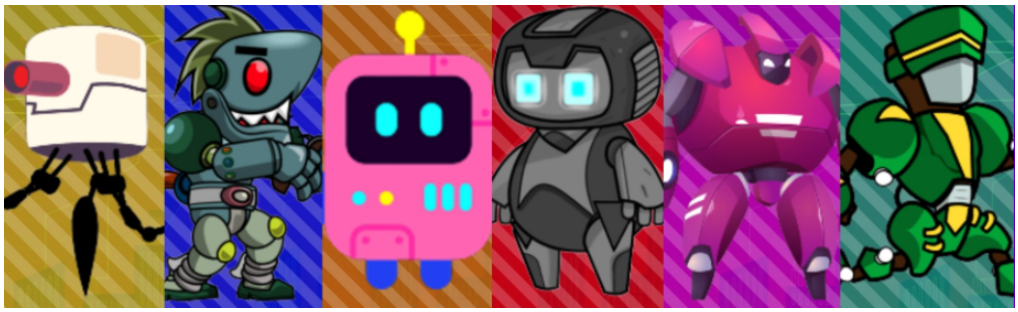


(a) **(b)**

Fonte: Elaboração própria.

A Figura 12 ilustra, da esquerda para a direita, os membros da Liga dos Robôs: Inspetor, Turbo, Charla, Timmy, Rosa e Andy, respectivamente.

Figura 12 – Imagens que representam os personagens da Liga dos Robôs.



Fonte: Adaptado de Itch.io (2026).

5.2 História dos Personagens

A seguir, são apresentados os esboços narrativos dos seis personagens propostos, elaborados com o objetivo de orientar a construção de suas trajetórias, personalidades e respectivas interações no contexto do jogo.

História do Robô Andy: Andy é o robô responsável por liderar a equipe de heróis. Em sua história, ele foi encurralado pelo vírus Ômega em uma batalha, onde se viu incapaz de combatê-lo sozinho. Com isso, o robô se escondeu em um cofre de senhas da cidade de Encrypta para se proteger, e somente uma senha super forte pode retirar o herói de dentro do artefato. A missão do jogador é controlar Andy pelo cenário, evitando os inimigos enquanto captura esferas de energia que contêm letras, números e caracteres especiais para formar uma senha super forte e retirá-lo de dentro do cofre. Inicialmente, Andy possui cinco corações de vida. Ao encostar em um inimigo, sua vida é reduzida em um coração, sendo derrotado caso perca todos os corações.

História da Robô Rosa: A robô Rosa é a heroína da liga responsável por monitorar os meios de comunicação da cidade, afetados pelo ataque do vírus malicioso. Durante os ataques à Encrypta, ela recebeu uma série de mensagens estranhas em sua caixa de e-mail. Rosa precisa da ajuda do jogador para identificar os e-mails de *phishing*, mensagens fraudulentas que cibercriminosos utilizam visando enganar suas vítimas e roubar seus dados (SOUZA; TANAKA, 2023). Os jogadores são apresentados a uma seleção de três e-mails, dentre os quais devem identificar e selecionar aquele correspondente a um ataque de *phishing*. Caso selecionem um e-mail legítimo, perdem um ponto de vida. Cada jogador possui três vidas ao longo da fase.

História do Robô Turbo: Os documentos mais importantes de Encrypta são guardados no explorador de arquivos, uma enorme pista de corrida cibernética que comporta os arquivos de todos os moradores da cidade. Esta pista é protegida pelo poderoso robô Turbo, que possui a habilidade de se transformar em um carro e percorrê-la em segundos, protegendo-a de todo e qualquer perigo iminente. Durante os ataques à Encrypta, o robô Turbo é responsável por se dirigir ao explorador e verificar se existem pastas infectadas. A missão do jogador é ajudá-lo a percorrer o local, recolhendo as pastas que ainda não foram comprometidas. Durante a fase, os jogadores encontram uma variedade de pastas de arquivos espalhadas pela pista. Eles devem evitar os inimigos e as pastas que possam conter arquivos maliciosos, como pastas de anexos de e-mails desconhecidos e jogos piratas, e coletar as seguras, como pastas de trabalhos escolares, receitas culinárias e documentos importantes para concluir a fase. Ao colidir com inimigos, o jogador perde uma vida, tendo, inicialmente, três corações disponíveis. Já ao coletar uma pasta maliciosa, o jogador reduz uma unidade na contagem de pastas seguras coletadas.

História do Robô Inspetor: O robô Inspetor é responsável por manter a segurança de todos os sites da cidade de Encrypta, em especial o da prefeitura, que é o mais acessado pelos moradores da região. Ele possui a habilidade de se multiplicar para facilitar a inspeção dos sites. Em sua história, ele foi *hackeado* pelo vírus inimigo e várias cópias maliciosas foram espalhadas pelo site da prefeitura. A missão do jogador é encontrar as cópias do robô que estão espalhadas em partes do site que indicam que ele não é seguro, como, por exemplo, *URLs* com *Hypertext Transfer Protocol (HTTP)*, falta de *Secure Sockets Layer (SSL)*, imagens de baixa qualidade, erros textuais, entre outros aspectos que podem auxiliar na detecção de sites fraudulentos. Os jogadores possuem três vidas e perdem uma a cada elemento inofensivo clicado no site.

História do Robô Timmy: O robô Timmy é responsável por manter e atualizar os arquivos de *backups* de todos os sistemas da cidade e também dos heróis da liga dos robôs. Em sua história, ele foi procurado por diversos moradores da cidade que temiam a infecção ao acessarem o site da prefeitura para se manterem informados sobre os ataques à Encrypta, em consequência dos ataques sofridos pelo robô Inspetor. Timmy possui arquivos de *backups* de versões anteriores do amigo e parte em uma missão para capturar

suas cópias maliciosas, a fim de restaurá-las para versões não infectadas. Nesta fase, os jogadores controlam Timmy, cujo objetivo é capturar as cópias infectadas do robô Inspetor e levá-las até a pasta de *backup* para recuperá-las. Inimigos com padrões de movimentação distintos aparecerão no cenário para impedir a progressão do jogador. Assim como nas fases anteriores, três vidas estão disponíveis ao iniciar.

História da Robô Charla: Charla é a pesquisadora da liga e é responsável por realizar novas descobertas que auxiliem a cidade e os robôs no combate aos crimes cibernéticos. Em sua mais recente pesquisa, Charla descobre que, para derrotar o vírus malicioso, é necessário responder a algumas perguntas sobre cibersegurança que somente os robôs da liga e pessoas que se protegem dos perigos da internet conseguem responder. Com isso, a heroína parte para o *firewall*, um poderoso mecanismo de proteção da região que contém as perguntas capazes de salvar a cidade. O desafio do jogador é responder ao *quiz* descoberto por Charla para restaurar a paz em Encrypta. Durante a aplicação da atividade, essa fase foi bloqueada, pois os estudantes realizaram os testes pré e pós-intervenção em formato físico, sem a necessidade de interação com esse nível.

O jogo possui um sistema de vidas desenvolvido para aumentar progressivamente o nível de dificuldade ao longo das fases. Inicialmente, o jogador começa a primeira fase com cinco vidas disponíveis. À medida que avança para as fases seguintes, a quantidade de vidas é reduzida gradualmente, tornando os desafios mais complexos e exigindo maior atenção e conhecimento por parte do jogador.

Caso o usuário perca todas as vidas disponíveis durante as fases, o sistema interromperá a partida e apresentará a opção de uma nova tentativa. Ao selecioná-la, o jogador poderá reiniciar o desafio, exceto na sexta fase, que não possui sistema de vidas.

5.3 Tópicos em Cibersegurança Abordados pelo Jogo

Os tópicos em cibersegurança escolhidos para serem abordados em cada uma das fases do jogo são apresentados a seguir.

Na primeira fase, os jogadores acompanham a história do robô Andy em uma dinâmica de jogo de plataforma, por meio da qual são abordados conceitos relacionados à criação de senhas seguras. Inicialmente, são apresentados aos fundamentos que caracterizam uma senha forte, a qual deve possuir um número mínimo de caracteres, incluindo letras, números e caracteres especiais, com o objetivo de aumentar a proteção das informações pessoais. Essa etapa fundamenta-se na habilidade EF07CO07 da BNCC, que propõe a identificação de problemas relacionados à segurança cibernética e o desenvolvimento de estratégias para proteger dados e informações. O *design* dessa fase é apresentado na Figura 13.

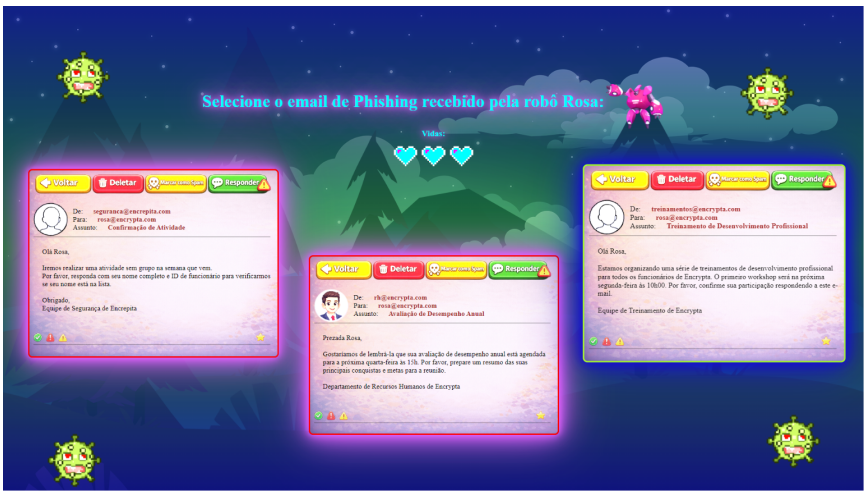
Figura 13 – Captura de tela: Fase do robô Andy.

Fonte: Elaboração própria.

Na segunda fase, a narrativa da robô Rosa é explorada em um jogo do gênero quebra-cabeça, cujo objetivo é desenvolver nos participantes a capacidade de identificar e reconhecer tentativas de *phishing* por meio de e-mails fraudulentos. Conforme apresentado na Figura 14.

O objetivo de aprendizagem desta etapa é evidenciar a importância de reconhecer possíveis ataques cibernéticos e verificar a confiabilidade das informações recebidas na internet. Essa etapa está fundamentada nas habilidades EF04CO08 e EF05CO08, que incentivam o desenvolvimento de práticas seguras e responsáveis no uso das tecnologias digitais, bem como a análise crítica das informações disponíveis em ambientes virtuais.

Figura 14 – Captura de tela: Fase da robô Rosa.



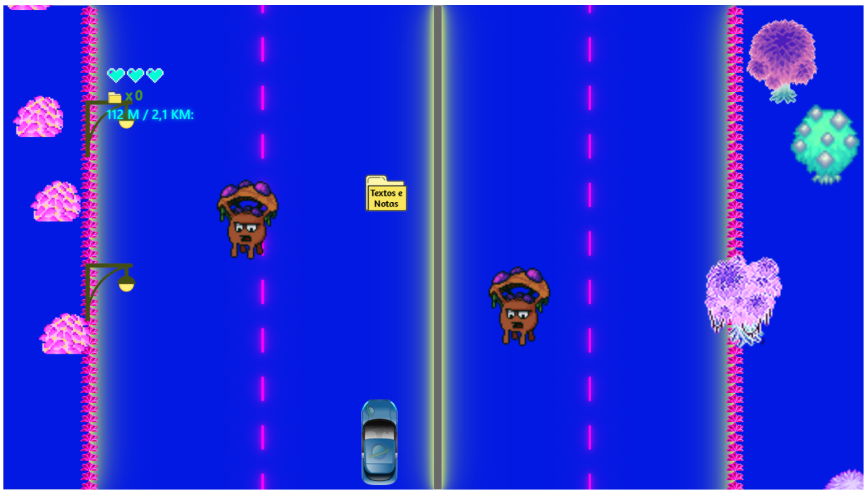
Fonte: Elaboração própria.

Na terceira fase, o foco recai sobre o robô Turbo, que conduz os jogadores em um jogo de corrida *top-down*, ensinando-os a reconhecer pastas de arquivos maliciosos. A Figura

15 apresenta a composição visual da fase.

Por meio da apresentação de diferentes formatos de arquivos, os jogadores desenvolvem habilidades relacionadas à identificação e categorização de arquivos, além do reconhecimento de pastas e arquivos potencialmente maliciosos. Essa atividade fundamenta-se nas habilidades EF06CO08 e EF05CO06, que destacam a importância de os estudantes aprenderem a armazenar, manipular, organizar, compactar e recuperar arquivos, documentos e seus metadados.

Figura 15 – Captura de tela: Fase do robô Turbo.

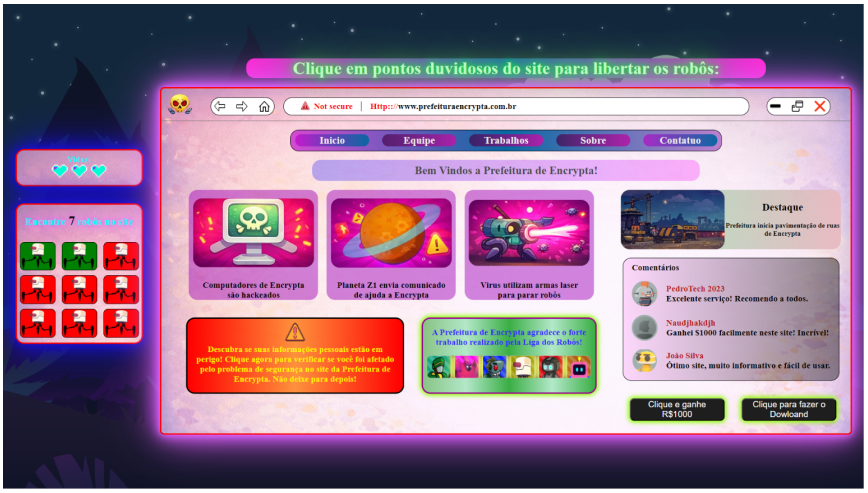


Fonte: Elaboração própria.

Em seguida, na quarta fase, a história do robô Inspetor é explorada em um quebra-cabeça interativo, que auxilia os participantes a detectar sites fraudulentos. Conforme ilustra a Figura 16.

A aprendizagem ocorre por meio da resolução de desafios interpretativos, nos quais o jogador deve identificar características comuns de tentativas de fraude, como imagens suspeitas, erros ortográficos e mensagens que solicitam o clique em *links* ou apresentam outros elementos que despertem desconfiança. Essa etapa também está fundamentada nas habilidades EF04CO08 e EF05CO08, que enfatizam a importância de distinguir, de forma crítica, conteúdos confiáveis daqueles que apresentam indícios de fraude ou desinformação.

Figura 16 – Captura de tela: Fase do robô Inspetor.



Fonte: Elaboração própria.

Na quinta fase, os jogadores auxiliam o robô Timmy em um jogo de plataforma que aborda a importância de armazenar arquivos de *backup* para a recuperação de dados em situações de perda. O *design* adotado para a fase pode ser visualizado na Figura 17.

De forma lúdica, os jogadores são convidados a compreender a importância da realização de *backups* como estratégia para garantir a recuperação de dados em caso de comprometimento das informações. Ao longo da atividade, os participantes podem perceber que a manutenção de cópias de segurança contribui significativamente para a preservação e recuperação de arquivos importantes. Assim como a atividade relacionada ao gerenciamento de arquivos, esta etapa também está fundamentada nas habilidades EF06CO08 e EF05CO06, que abordam competências relacionadas ao armazenamento, à organização e à recuperação de dados.

Figura 17 – Captura de tela: Fase do robô Timmy.

Fonte: Elaboração própria.

Por fim, na sexta fase, protagonizada por Charla, os participantes respondem a um *quiz* composto por 15 questões de múltipla escolha (com três a quatro alternativas por questão), que tem o objetivo de avaliar os conhecimentos adquiridos ao longo do jogo. A Figura 18 apresenta a composição visual da fase.

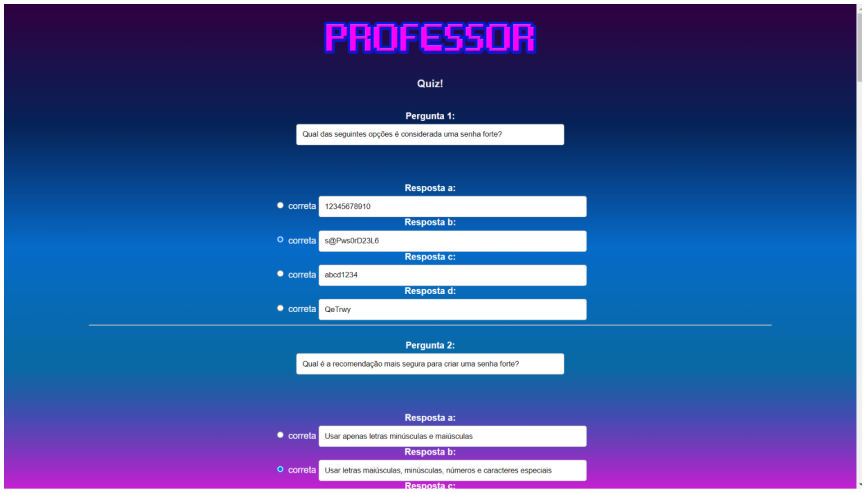
Figura 18 – Captura de tela: Fase da robô Charla.

Fonte: Elaboração própria.

5.4 Área do Professor

A área do professor é protegida por senha e permite ao educador editar o *quiz* presente na fase final do jogo, possibilitando a personalização das perguntas de acordo com os conteúdos trabalhados em sala de aula e os objetivos da atividade. Como as fases apresentam desafios independentes, cada uma abordando um tema específico de cibersegurança, o professor pode utilizar uma determinada fase como recurso didático para trabalhar um conteúdo específico e, posteriormente, configurar o *quiz* final com perguntas relacionadas ao tema abordado. Dessa forma, a funcionalidade permite adaptar a avaliação ao conteúdo explorado em cada aula. A Figura 19 apresenta a interface dessa funcionalidade.

Figura 19 – Captura de tela referente à área do professor.



Fonte: Elaboração própria.

5.5 Instrumentação e Recursos de Implementação

Na fase de implementação, foram selecionadas as ferramentas necessárias para atender aos requisitos definidos na metodologia do projeto. Optou-se pelo desenvolvimento em web, utilizando HTML, CSS e JavaScript para a construção do jogo proposto.

O *port*[1] para *desktop* foi realizado utilizando o *framework* Electron, permitindo a execução do jogo em ambientes Linux e Windows. A realização do *port* para o macOS tornou-se inviável devido às restrições do ecossistema Apple, que incluem a necessidade de *hardware* proprietário, o custo anual de adesão ao programa de desenvolvedores da empresa, bem como a obrigatoriedade de submissão e homologação rigorosa pela App Store.

O *port* para dispositivos móveis foi realizado utilizando o Android Studio, possibilitando a disponibilização do jogo em formato *Android Package Kit* (APK) para download. Quanto à viabilidade de um *port* para o iOS, esta foi considerada impraticável devido às mesmas restrições do ecossistema Apple já detalhadas para o sistema macOS.

Além disso, o jogo foi disponibilizado em ambiente online por meio dos servidores do Itch.io, podendo ser acessado diretamente em sua página oficial, sem a necessidade de download (ABREU, 2026).

Quanto aos *sprites*[2] dos personagens, foram utilizados *assets*[3] disponibilizados gra-

[1] O termo *port* (ou *porting*) refere-se ao processo de adaptação de um *software* para que possa ser executado em um ambiente, plataforma ou *hardware* diferente daquele para o qual foi originalmente desenvolvido.

[2] *Sprites* são imagens bidimensionais (2D) utilizadas na renderização de personagens e objetos dentro do ambiente de um jogo.

[3] *Assets* são recursos digitais que compõem um jogo, como modelos 3D, texturas, sons e elementos de interface.

tuitamente pela plataforma de distribuição de jogos independentes (Itch.io, 2026). Já a trilha sonora do jogo foi composta por músicas e efeitos sonoros obtidos em repositórios de conteúdo gratuito (MixKit, 2026; Chosic, 2026).

As tecnologias utilizadas no processo de desenvolvimento do jogo estão listadas na Tabela 7, incluindo a versão utilizada e onde foram empregadas.

Tabela 7 – Instrumentação tecnológica e suas versões.

Ferramenta / Tecnologia	**Versão**	**Função no Projeto**
JavaScript (Vanilla JS)	ES6+	Lógica principal, mecânicas do jogo e manipulação do DOM.
HTML5 / CSS3	W3C Standard	Estruturação de conteúdo e interface visual responsiva.
Node.js	v22.18.0	Ambiente de execução para ferramentas de *build* e pacotes.
Electron	v32.3.3	*Framework* para portabilidade e execução *Desktop*.
Android Studio (SDK)	API 36 (v16)	Compilação e geração do pacote (APK) para dispositivos móveis.
Itch.io	Web/Cloud	Distribuição e gestão do histórico de *builds* executáveis.

Fonte: Elaboração própria.

5.6 Proposta de Utilização em Contexto Educacional

Esta seção apresenta uma proposta de utilização do jogo em contexto escolar, oferecendo aos professores um roteiro de aplicação que pode ser adaptado de acordo com os objetivos da disciplina, o perfil da turma e o tempo disponível. Ressalta-se que esta proposta constitui uma sugestão de uso pedagógico, podendo ser modificada conforme as necessidades de cada contexto educacional.

5.6.1 Público-alvo e Contexto de Aplicação

O público-alvo da ferramenta compreende estudantes da educação básica, sendo recomendada sua utilização entre estudantes do 4º e do 9º ano do Ensino Fundamental. O jogo aborda conteúdos relacionados à cibersegurança, podendo ser utilizado como recurso

complementar às atividades desenvolvidas em sala de aula, sem substituir a atuação do professor ou as estratégias pedagógicas adotadas.

5.6.2 Estratégia Pedagógica do Jogo

O processo de aprendizagem proposto pelo jogo baseia-se na aprendizagem ativa, em que o estudante constrói o conhecimento por meio da resolução de desafios, da reflexão sobre suas decisões e da interação contínua com a aplicação. Em vez de apenas transmitir informações, o jogo incentiva a participação ativa do estudante na resolução de problemas contextualizados, permitindo que os conceitos de cibersegurança sejam construídos ao longo da interação com as diferentes mecânicas e cenários propostos.

Ao longo das fases, os estudantes recebem *feedback* imediato sobre suas ações, permitindo identificar erros, compreender suas consequências e ajustar suas estratégias de resolução. Além disso, o sistema de vidas e a possibilidade de repetir as fases favorecem a aprendizagem por tentativa e erro, incentivando a revisitação dos desafios e o reforço gradual dos conceitos trabalhados.

A progressão linear do jogo, com aumento gradual da dificuldade, possibilita que os conteúdos sejam apresentados de forma incremental, respeitando uma sequência de complexidade crescente. Paralelamente, a narrativa e os personagens contextualizam os desafios em situações fictícias inspiradas em problemas reais de segurança digital, favorecendo a associação entre os conceitos aprendidos no jogo e situações que os estudantes podem vivenciar em seu cotidiano.

5.6.3 Sequência Didática Sugerida

O jogo foi desenvolvido de forma modular, em que cada fase aborda um tema específico da área de cibersegurança. Essa característica permite que o professor selecione apenas a fase relacionada ao conteúdo trabalhado em determinada aula, adaptando a utilização da ferramenta às necessidades da turma.

Como exemplo, a Fase 2 aborda a identificação de tentativas de *phishing*. Nesse contexto, o professor pode desenvolver uma aula voltada à identificação de fraudes eletrônicas e, posteriormente, utilizar essa fase do jogo para reforçar os conceitos apresentados. Antes da aplicação, o educador pode editar as questões presentes no *quiz* da última fase, personalizando-as de acordo com o conteúdo trabalhado em sala de aula.

Da mesma forma, as demais fases podem ser utilizadas como apoio ao ensino de diferentes tópicos de cibersegurança. A possibilidade de personalização do *quiz* permite que a avaliação final seja alinhada aos conteúdos efetivamente abordados em cada aula.

Considerando essas características, sugere-se a seguinte sequência didática.

Etapa 1 - Exposição ao Tema

Inicialmente, o professor apresenta os conceitos relacionados ao conteúdo que será trabalhado na aula, discutindo os riscos associados ao tema e destacando sua importância para a segurança no ambiente digital. Nesse momento, também podem ser realizadas atividades diagnósticas para identificar os conhecimentos prévios dos estudantes, bem como suas experiências relacionadas ao uso da internet e das tecnologias digitais. Além disso, o docente pode estimular a participação dos estudantes por meio do compartilhamento de situações cotidianas relacionadas ao assunto, favorecendo a conexão entre os conceitos abordados e as experiências vivenciadas pelos participantes.

Etapa 2 - Contextualização da Narrativa

Antes do início da interação com o jogo, recomenda-se que o professor apresente brevemente a narrativa da aplicação, contextualizando a cidade de Encrypta, os personagens, os robôs da liga e os desafios enfrentados ao longo da história. Essa contextualização favorece a imersão dos estudantes, desperta o interesse pela atividade e auxilia na compreensão dos objetivos da missão que será realizada.

Etapa 3 - Interação com o Jogo

Após a contextualização, os estudantes interagem com a fase correspondente ao conteúdo trabalhado. Como as fases são independentes e apresentam mecânicas simples, o tempo necessário para compreender sua dinâmica é reduzido, permitindo sua utilização durante uma aula convencional. Em média, cada fase pode ser concluída em aproximadamente dez minutos, embora esse tempo possa variar de acordo com a faixa etária, o nível de letramento digital e o ritmo de aprendizagem dos estudantes.

Durante essa etapa, recomenda-se que o professor acompanhe a atividade, esclarecendo dúvidas, auxiliando na compreensão das mecânicas e incentivando os estudantes a explorarem a narrativa e os desafios propostos. Caso necessário, as fases podem ser repetidas, permitindo a revisão dos conteúdos e o aperfeiçoamento do desempenho.

Etapa 4 - Discussão, Reflexão e Avaliação da Aprendizagem

Ao término da interação com o jogo, os estudantes podem ser convidados a refletir sobre os conteúdos abordados durante a atividade. Inicialmente, o professor pode promover uma discussão sobre a narrativa do jogo, incentivando os alunos a interpretar as ações dos personagens e o papel desempenhado por cada integrante da Liga dos Robôs na proteção da cidade. Questões como “Qual era a função de cada personagem na Liga dos Robôs?”, “Qual ameaça cada personagem ajudava a combater?” e “Por que cada um deles era

importante para proteger a cidade?" podem estimular a compreensão da narrativa e sua relação com os conceitos de cibersegurança. Em seguida, o professor pode conduzir uma discussão mais ampla utilizando perguntas como: "Quais ameaças foram encontradas?", "Quais práticas podem ser adotadas para evitá-las?" e "Como essas situações se relacionam com experiências vivenciadas no cotidiano?". Essa discussão favorece a conexão entre os desafios enfrentados no ambiente do jogo e situações reais do contexto digital, contribuindo para a consolidação dos conhecimentos trabalhados durante a atividade.

Esse momento favorece a consolidação da aprendizagem, estimulando o pensamento crítico e a associação entre os desafios encontrados no jogo e situações reais enfrentadas pelos estudantes. Além da discussão coletiva, recomenda-se a utilização de mecanismos de avaliação, como o *quiz* personalizável da última fase, testes de conhecimento ou outras atividades compatíveis com os objetivos da aula, permitindo verificar a aprendizagem dos estudantes.

Etapa 5 - Continuidade e Aprofundamento

Após a conclusão da atividade, recomenda-se a retomada dos conteúdos em aulas posteriores por meio de estratégias complementares, como debates, estudos de caso, análise de situações reais ou elaboração de materiais pelos próprios estudantes. Essas atividades podem favorecer a reflexão sobre os conceitos abordados e contribuir para a consolidação dos conhecimentos construídos durante a experiência com o jogo.

5.6.4 Recomendações de Uso em Contextos Educacionais

Conforme apresentado, este material de apoio educacional tem como finalidade servir como um guia para auxiliar a aplicação da ferramenta em contextos educacionais. Entretanto, recomenda-se que sua utilização seja realizada em conjunto com as diretrizes e os materiais pedagógicos oficiais previstos pela BNCC, a fim de garantir o adequado planejamento e direcionamento das atividades propostas (BRASIL - Ministério da Educação, 2022).

Além disso, ressalta-se que a mediação do professor desempenha papel fundamental durante todo o processo de utilização da ferramenta. Cabe ao educador contextualizar os conteúdos abordados, esclarecer dúvidas, relacionar as situações simuladas no jogo ao cotidiano dos estudantes e incentivar discussões que promovam a reflexão crítica sobre os riscos presentes no ambiente digital. Dessa forma, a aplicação deve ser compreendida como um recurso complementar às práticas pedagógicas, potencializando o processo de ensino e aprendizagem.

Este capítulo apresentou os principais aspectos relacionados ao *design* e ao desenvolvimento do jogo, incluindo a apresentação da narrativa e personagens, os conteúdos de cibersegurança abordados, as mecânicas propostas e as ferramentas utilizadas durante

sua implementação. Esses elementos constituem a aplicação proposta, cuja avaliação será apresentada no próximo capítulo, juntamente com os procedimentos adotados e a análise dos resultados obtidos durante sua aplicação.

Capítulo 6

Análise dos Resultados e Discussões

Este capítulo apresenta e discute os resultados obtidos ao longo do processo de avaliação da proposta. Inicialmente, são apresentados os resultados do estudo piloto, conduzido por meio de uma PoC, cujo objetivo foi verificar a viabilidade e a aplicabilidade da ferramenta, permitindo a identificação de limitações e a realização de ajustes antes da condução do estudo principal.

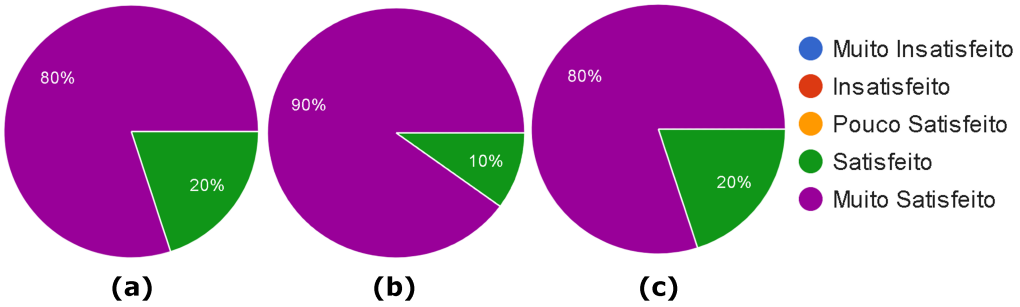
Em seguida, são descritos o perfil dos participantes e os procedimentos adotados na aplicação da pesquisa realizada com estudantes do CAp/UFU, organizados por meio dos questionários de pré e pós-teste, a aplicação do modelo de avaliação MEEGA+, a análise de *logs* de interação com a ferramenta e, por fim, a observação direta em sala de aula. As análises buscam responder às questões de pesquisa desta dissertação, cruzando o desempenho objetivo com a percepção do aprendizado, engajamento e motivação dos participantes.

6.1 Prova de Conceito do Jogo Encrypta

A versão para a PoC do jogo foi parcialmente publicada e apresentada em (ABREU; MIANI; NOMURA, 2024). O estudo foi realizado por meio da divulgação do jogo em redes sociais, onde obteve-se a participação de 10 usuários, com idades entre 12 e 25 anos, que jogaram o jogo e responderam ao *quiz* presente na última fase. Os participantes também foram convidados a responder a um pequeno formulário composto por 9 questões fundamentadas no modelo MEEGA+.

As questões do questionário foram avaliadas por meio de uma escala Likert, variando de “muito insatisfeito” a “muito satisfeito”. Conforme observado na Figura 20, 80% dos participantes demonstraram estar muito satisfeitos com o visual do jogo apresentado. Além disso, 90% reconheceram que o jogo possui potencial para alertar os usuários sobre os perigos da internet, e 80% afirmaram que o recomendariam a outras pessoas.

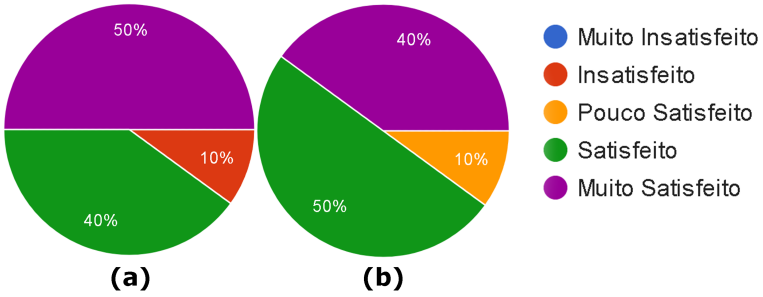
Figura 20 – a) O visual do jogo é atraente, interessante? b) Ele pode alertar sobre os perigos da internet? c) Recomendaria o jogo?



Fonte: Elaboração própria.

Quando questionados sobre a facilidade de uso e interação com o jogo, alguns pontos de atenção foram destacados. Observando a Figura 21, cerca de 10% dos participantes demonstraram insatisfação, indicando que o jogo pode apresentar dificuldades para pessoas que nunca tiveram contato com jogos digitais, evidenciando a possível necessidade de auxílio de terceiros durante a utilização. Além disso, 10% dos jogadores mostraram-se pouco satisfeitos com a facilidade de uso e compreensão do jogo.

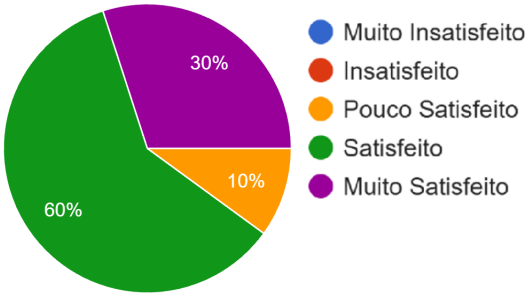
Figura 21 – a) O jogo acolhe pessoas de diferentes niveis de experiência com jogos digitais? b) O jogo é fácil de usar/entender?



Fonte: Elaboração própria.

Os participantes também foram questionados quanto à capacidade do jogo de prender sua atenção durante a atividade. Cerca de 10% dos participantes relataram estar pouco satisfeitos com essa afirmação e apenas 30% atribuíram a nota máxima a esse quesito, conforme apresentado na Figura 22.

Figura 22 – O jogo mantém a minha atenção?



Fonte: Elaboração própria.

Por fim, ao analisar os resultados obtidos no *quiz*, observou-se que 2 jogadores cometeram apenas 1 erro, 1 jogador cometeu 2 erros e outro cometeu 3 erros. Além disso, todos os demais participantes responderam corretamente às 15 questões apresentadas, indicando um bom desempenho no *quiz* relacionado aos tópicos de cibersegurança abordados no jogo. Esses resultados sugerem que os participantes apresentaram domínio sobre os conteúdos avaliados durante a atividade. A Figura 23 apresenta a relação de erros e acertos por jogador.

Figura 23 – Relação de erros e acertos por jogador.

	Jogadores									
Perguntas	1	2	3	4	5	6	7	8	9	10
1	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
2	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
3	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro	Acerto
4	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
5	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
6	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Erro	Acerto	Acerto	Acerto
7	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
8	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
9	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
10	Acerto	Acerto	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
11	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
12	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro	Acerto
13	Acerto	Erro	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Erro
14	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto
15	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto	Acerto

Fonte: Elaboração própria.

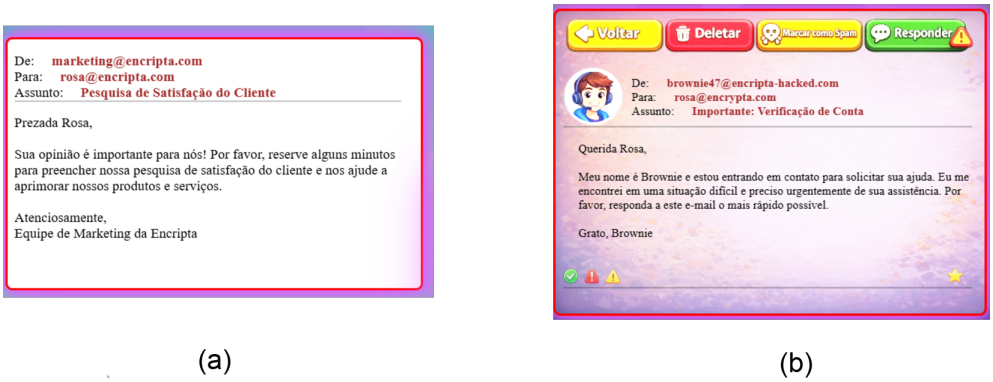
É importante destacar que esta PoC se caracteriza como um estudo preliminar que não teve o objetivo de avaliar o ganho de conhecimento decorrente do uso do jogo proposto. O fato de o estudo ter sido conduzido em ambiente online possibilita o uso de fontes externas durante a resolução das questões, o que comprometeria a confiabilidade dos dados. Em contrapartida, os resultados da PoC foram importantes para compreender a viabilidade da proposta e identificar problemas de *design*, apresentados na subseção a seguir.

6.1.1 Alterações de *design*

Com base nos *feedbacks* coletados durante o desenvolvimento da PoC, foram realizadas melhorias no jogo com o objetivo de refinar a proposta e aprimorar aspectos identificados como oportunidades de melhoria. Dentre os pontos de maior destaque do estudo piloto, os participantes evidenciaram o visual atraente apresentado pelo jogo. Com o intuito de aprimorar ainda mais a interface e os menus, foram realizadas melhorias na parte gráfica, visando refinar a proposta.

Dentre as melhorias, destacam-se ajustes gráficos voltados à interface, incluindo a padronização de elementos e a adição de componentes como sombras e texturas, que remetem à estética futurista proposta. Essas melhorias podem ser observadas na Figura 24, que ilustra as alterações na interface da caixa de e-mail da fase de detecção de *phishing*. Entre as mudanças, destacam-se a implementação de planos de fundo, a centralização de elementos, a inserção de ícones e botões, bem como a inclusão de fotos de perfil para os remetentes das mensagens.

Figura 24 – Capturas de tela: a) Primeira versão das caixas de emails b) Versão final das caixas de emails.



(a) (b)

Fonte: Elaboração própria.

Além da padronização de ícones e elementos na tela, também foram realizadas melhorias textuais, incluindo correções de erros de ortografia e acentuação. Adicionalmente, foram implementadas melhorias no sistema de vidas, a adição de níveis de dificuldade em determinadas fases e a correção de erros gerais.

Como exemplo, destaca-se o ajuste realizado na representação de senhas seguras apresentado na Figura 25, que anteriormente apresentava apenas oito espaços para caracteres, o que não condiz com boas práticas de cibersegurança, que recomendam senhas com pelo menos 12 caracteres. Essas melhorias foram aplicadas com o objetivo de aprimorar a experiência geral do jogador.

Figura 25 – Capturas de tela: a) Versão inicial do contador de senhas b) Versão final do contador de senhas.

(a) (b)

Fonte: Elaboração própria.

Entre os pontos de atenção apresentados pelos jogadores, destacaram-se questões relacionadas à dificuldade de uso, bem como às possíveis barreiras enfrentadas por usuários com diferentes níveis de familiaridade com jogos digitais. Com base nesses *feedbacks*, foram realizadas melhorias com o intuito de facilitar a compreensão dos usuários sobre os objetivos propostos, controles e possibilidades de utilização.

A Figura 26 apresenta algumas dessas melhorias. Nela, é possível observar a adição de instruções antes do inicio de cada fase, recurso que não estava presente na versão anterior. Além disso, em fases de plataforma, o jogo iniciava automaticamente ao clicar em "jogar", o que poderia gerar confusão entre os jogadores. Com a alteração implementada, essas fases passaram a ser iniciadas apenas mediante a interação explícita do usuário, indicando quando a fase deve começar.

Figura 26 – Capturas de tela: a) Ajuda da Fase 1 b) Ajuda da Fase 5.

(a) (b)

Fonte: Elaboração própria.

Por fim, foi destacado por uma parcela dos jogadores que o jogo poderia não ser suficientemente atrativo para manter sua atenção. Com base nisso, foram adicionados diversos elementos visuais à interface, além de aprimoramentos nas exibições textuais,

fontes, iluminação e apresentação dos elementos, bem como nos planos de fundo, conforme observado na Figura 27. Essas melhorias foram implementadas com o objetivo de aumentar o nível de engajamento dos participantes durante a interação com a ferramenta.

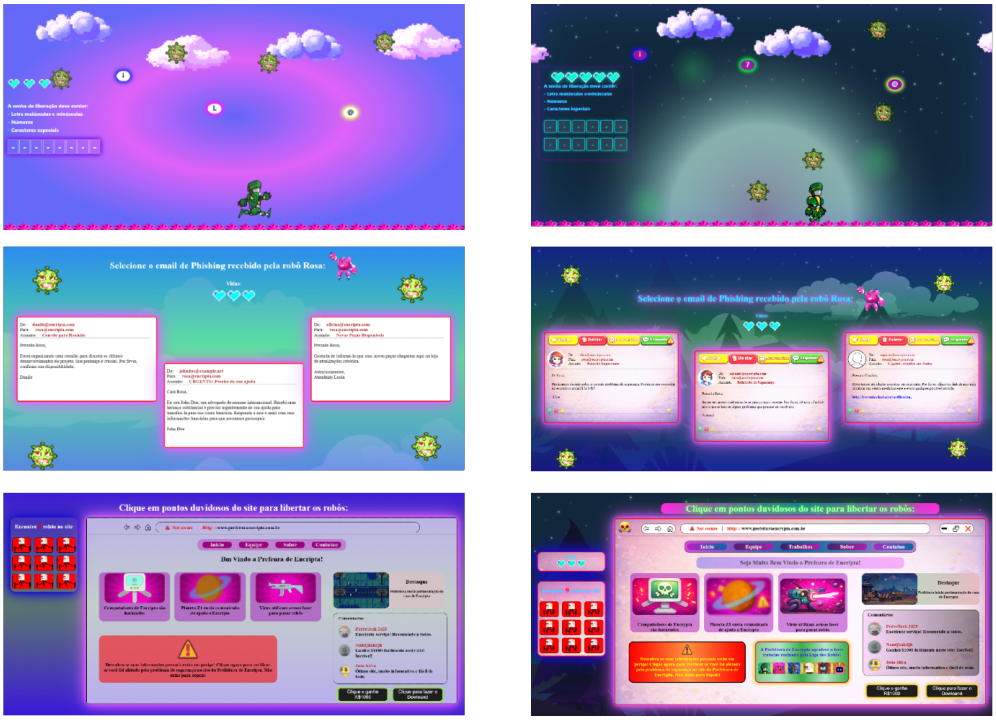
Figura 27 – Capturas de tela: a) Versão inicial da tela de personagens b) Versão final da tela de personagens.

(a) (b)

Fonte: Elaboração própria.

A Figura 28 apresenta o detalhamento em tela cheia das fases do jogo que passaram por mudanças mais significativas. É possível observar a evolução no que diz respeito à apresentação textual, à inclusão de elementos lúdicos na interface, à organização dos objetivos e ao sistema de vidas, dentre outros aspectos.

Figura 28 – Visão geral do jogo: a) Primeira versão b) Versão final.



(a) (b)

Fonte: Elaboração própria.

As sugestões coletadas a partir do *feedback* dos usuários foram utilizadas como base para o refinamento do *software*, orientando a identificação de ajustes relacionados à usabilidade, à experiência de uso, à apresentação dos objetivos e às formas de interação com a aplicação.

6.2 Perfil dos Participantes

Após a aplicação dos critérios de inclusão e exclusão, bem como a consolidação dos dados coletados durante a aplicação no CAp/UFU, a quantidade total de participantes deste estudo foi de 110 estudantes. Esses participantes estão distribuídos entre as 11 turmas envolvidas na pesquisa.

A Tabela 8 apresenta a caracterização da amostra, contemplando a distribuição dos estudantes por ano escolar, turma e faixa etária, informações relevantes para a análise dos resultados. A pesquisa contou com a participação de estudantes com idades entre 8 e 14 anos, dos quais 48,2% eram do sexo masculino e 51,8% do sexo feminino.

Tabela 8 – Caracterização da amostra final por ano escolar, turma e idade.

Ano Escolar	**Turma**	**Quantidade (N)**	**Média de Idade**
4º Ano	A	12	8,8
	B	13	9,1
	C	12	9,1
5º Ano	A	7	9,9
	B	11	10,1
	C	11	10,1
6º Ano	A	8	11,1
	B	5	11,4
	C	8	11
7º Ano	A	11	12,3
	B	12	12,3
Total Geral		**110**	

Fonte: Elaboração própria.

6.3 Planejamento e Aplicação das Atividades

A execução da intervenção seguiu as etapas previstas no roteiro de aplicação do estudo, sendo realizada conforme o planejamento proposto. No entanto, apesar do esforço em cumprir integralmente o roteiro, foram observadas algumas nuances durante sua execução.

A apresentação do projeto ocorreu conforme o planejado, com uma duração média de cinco minutos para cada turma, sendo esse tempo adequado para a introdução da

proposta e para o esclarecimento de dúvidas pontuais dos estudantes antes do início da atividade.

Durante as etapas de pré-teste, observou-se certa dificuldade por parte dos estudantes mais jovens, especialmente do 4º e 5º anos, em concluir o questionário no tempo estipulado. Em alguns casos, o tempo de 15 minutos foi ultrapassado.

Quanto ao tempo de uso do jogo, os estudantes dispuseram de 60 minutos para sua utilização. Como exceção, as turmas 5º A, 5º B e 6º A tiveram aproximadamente 35 minutos para utilizar a ferramenta. Como complemento, para as turmas que tiveram dois períodos disponíveis no laboratório, após a finalização de todos os testes, os estudantes eram liberados para voltar a interagir com o jogo, caso desejassem, o que pode ter ampliado o tempo de interação para além dos 60 minutos previstos no roteiro.

Já durante os testes pós-intervenção, a maioria dos estudantes conseguiu finalizar o pós-teste e o questionário MEEGA+ dentro do limite de 20 minutos estabelecido, o que pode ter sido influenciado pela não leitura completa das questões ou pela possibilidade de retornar à interação com o jogo.

6.4 Análise do Desempenho (Pré e Pós-teste)

Para a coleta dos dados, os estudantes foram convidados a responder a dois questionários, chamados de pré-teste e pós-teste, aplicados em momentos distintos da atividade. Os questionários foram compostos por 15 questões iguais, identificadas de Q1 a Q15. As questões Q1 a Q3 abordaram o tema do uso de senhas seguras; Q4 a Q7 trataram de e-mails de *phishing*; Q8 a Q11 contemplaram a detecção de arquivos e sites maliciosos; Q12 a Q14 enfocaram a importância de *backups*; e Q15, a segurança de dados online.

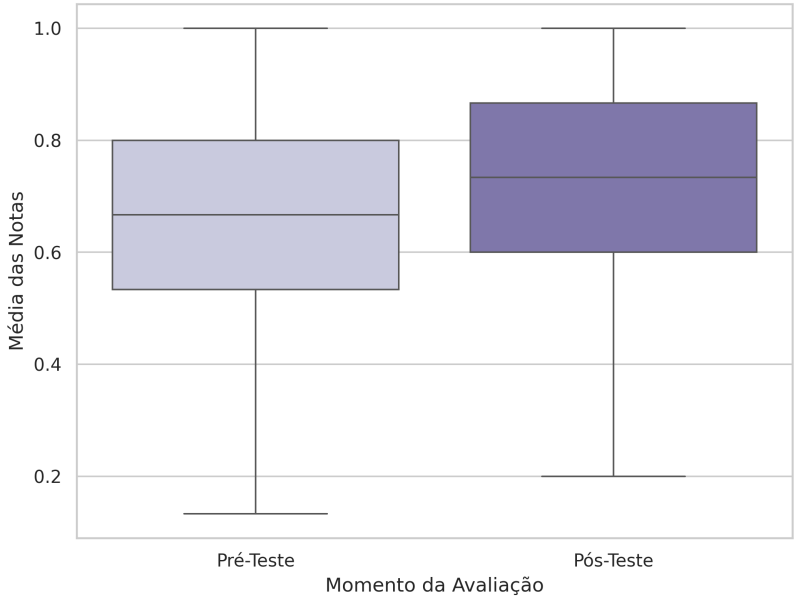
Inicialmente, avaliou-se a normalidade dos dados por meio do teste de Shapiro-Wilk, cujo resultado indicou violação da hipótese de normalidade ($p = 0{,}0004$). Em seguida, a homogeneidade das variâncias foi verificada pelo teste de Levene, que indicou variâncias homogêneas ($p = 0{,}1742$). Esses resultados justificaram a utilização de testes estatísticos não paramétricos nas análises subsequentes.

Ao analisar o desempenho geral dos participantes, observa-se um aumento no desempenho dos estudantes entre o pré-teste e o pós-teste. A mediana das notas passou de 0,67 no pré-teste para 0,73 no pós-teste, indicando uma melhora no desempenho após a aplicação da intervenção. Conforme ilustrado na Figura 29, verifica-se um deslocamento ascendente da distribuição das notas no pós-teste em relação ao pré-teste, evidenciado pelo aumento da mediana.

Esse resultado é corroborado pela diferença estatística apresentada pelo teste de Wilcoxon ($Z = 4,821$; $p < 0,001$). Como complemento, buscou-se compreender a magnitude desse impacto por meio do tamanho do efeito (r). O valor obtido ($r = 0,325$) indica um

efeito de magnitude média, demonstrando que o estudo promoveu um ganho de conhecimento entre os estudantes.

Figura 29 – Comparação de desempenho: pré *vs* pós-teste.



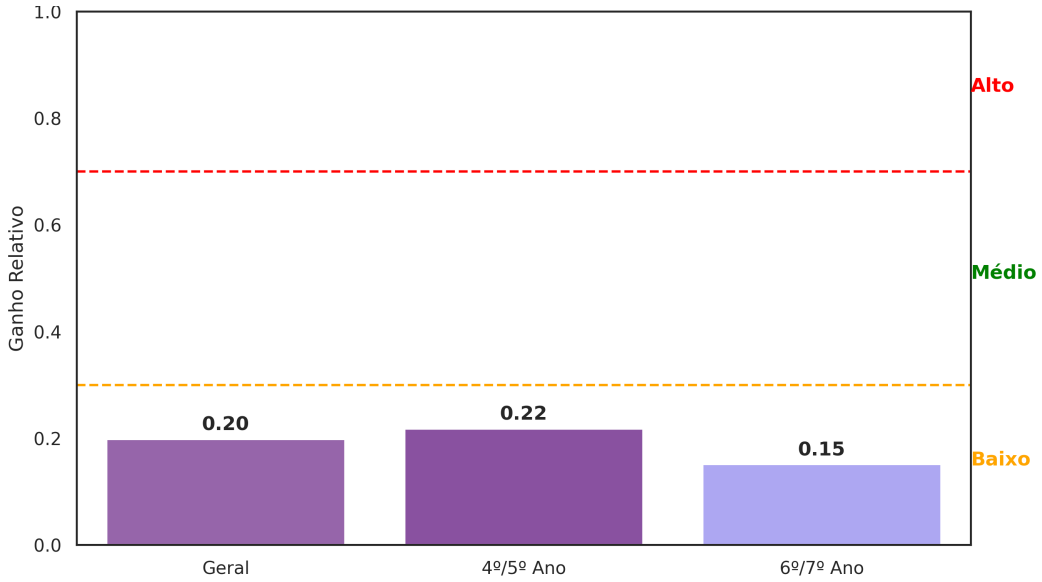
Fonte: Elaboração própria.

Utilizando a métrica de ganho de Hake, amplamente empregada na avaliação de ferramentas educacionais com intervenções baseadas em pré e pós-teste, foi possível observar que a intervenção resultou em baixo ganho de conhecimento para os estudantes, tanto de forma geral quanto na análise por ano escolar.

O desempenho geral foi de aproximadamente 20% (g = 0,20), enquanto as turmas do 4º e 5º anos apresentaram um desempenho ligeiramente superior, com cerca de 22% (g = 0,22). Por fim, os estudantes mais velhos, do 6º e 7º anos, obtiveram o menor desempenho, com aproximadamente 15% (g = 0,15).

Todos os resultados se enquadraram como baixo ganho de conhecimento, segundo a classificação da métrica de Hake. O desempenho pode ser visualizado na Figura 30.

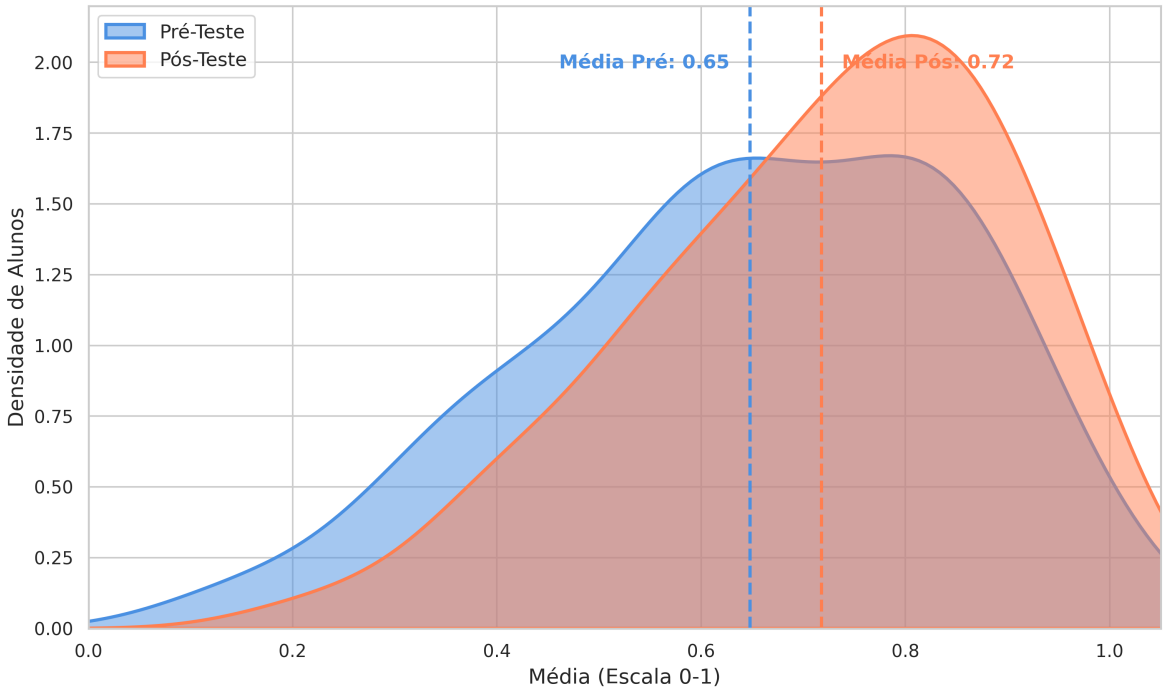
Figura 30 – Índice de Ganho de Hake.



Fonte: Elaboração própria.

Ao analisar a densidade das notas (Figura 31), é possível identificar fatores que ajudam a explicar o índice de Ganho de Hake classificado como baixo. Observa-se que, no pré-teste, os estudantes já apresentavam uma média de $0,65$, sugerindo que parte do conteúdo avaliado já era de conhecimento dos participantes antes da aplicação do estudo. Esse cenário reduz o potencial de crescimento capturado pelo ganho normalizado de Hake, uma vez que os participantes já iniciaram a atividade com um nível relativamente elevado de conhecimento. Ainda assim, observa-se um deslocamento da distribuição das notas para valores mais elevados no pós-teste, refletido pelo aumento da média para $0,72$. Esse comportamento indica uma melhora geral no desempenho dos estudantes, sugerindo que o jogo contribuiu para consolidar e ampliar os conhecimentos relacionados à cibersegurança.

Figura 31 – Distribuição de notas: pré *vs* pós-teste.

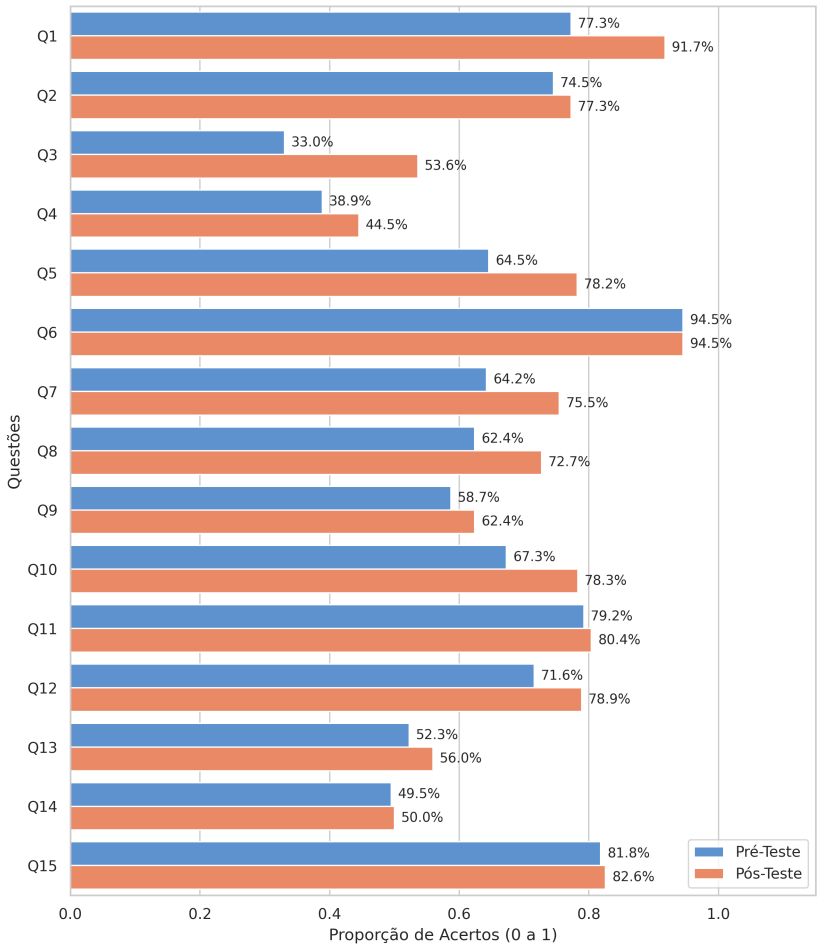


Fonte: Elaboração própria.

Para aprofundar a análise sobre o nível de conhecimento dos participantes, utilizou-se o teste de McNemar para verificar o desempenho individual em cada uma das 15 questões do instrumento. Observou-se uma melhora estatisticamente significativa ($p < 0,05$) nas questões Q1, Q3, Q5, Q8 e Q10, sugerindo uma associação entre a utilização do jogo e um melhor desempenho dos participantes nesses tópicos, sem que isso permita inferir, isoladamente, uma absorção definitiva dos conteúdos. Nas demais questões, embora as mudanças não tenham atingido significância estatística, notou-se um ganho incremental na taxa de acertos, conforme ilustrado na Figura 32.

É fundamental destacar que, em questões como a Q6 (que manteve um desempenho de $94,5\%$), além da Q11 e Q15, a estagnação observada corrobora os achados do Ganho de Hake. Nesses casos, os estudantes já apresentavam um domínio prévio elevado, restando pouco espaço para evolução no pós-teste. Assim, a estabilidade dos altos índices de acerto indica que os participantes já apresentavam domínio prévio desses conteúdos. Consequentemente, essas questões possuíam menor capacidade de detectar mudanças decorrentes da intervenção, devido ao possível efeito teto.

Figura 32 – Taxa de acerto por questão no pré e pós-teste.

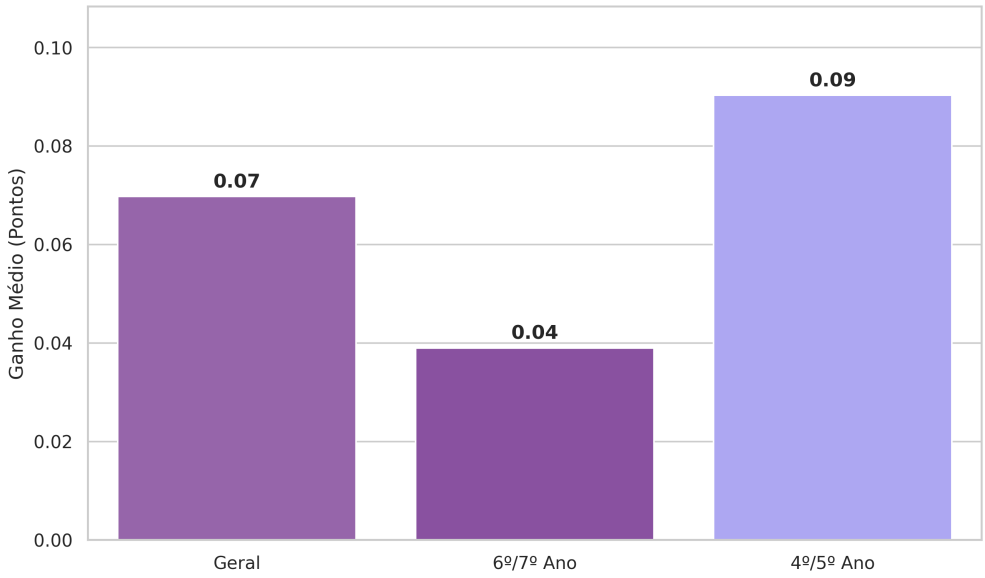


Fonte: Elaboração própria.

Ao analisar a melhora média do desempenho dos estudantes após a intervenção, é possível observar, na Figura 33, um aumento médio de 7% no desempenho do público em geral. Ao segmentar por ano escolar, verifica-se uma melhora média mais acentuada entre os estudantes mais novos, com cerca de 9%. Por outro lado, os estudantes mais velhos, do 6º ao 7º ano, apresentaram um desempenho inferior, com aproximadamente 4% de melhora.

Esse resultado pode ser explicado pela natureza comportamental dos estudantes mais novos, que, ao saberem que participariam de uma atividade com o jogo, podem ter respondido ao pré-teste com menos atenção. Já no pós-teste, possivelmente dedicaram mais atenção às questões, resultando em uma melhora mais expressiva. Além disso, os estudantes mais velhos podem já possuir uma maior familiaridade com a tecnologia, o que pode ter contribuído para um melhor desempenho no pré-teste e, consequentemente, uma menor variação no pós-teste.

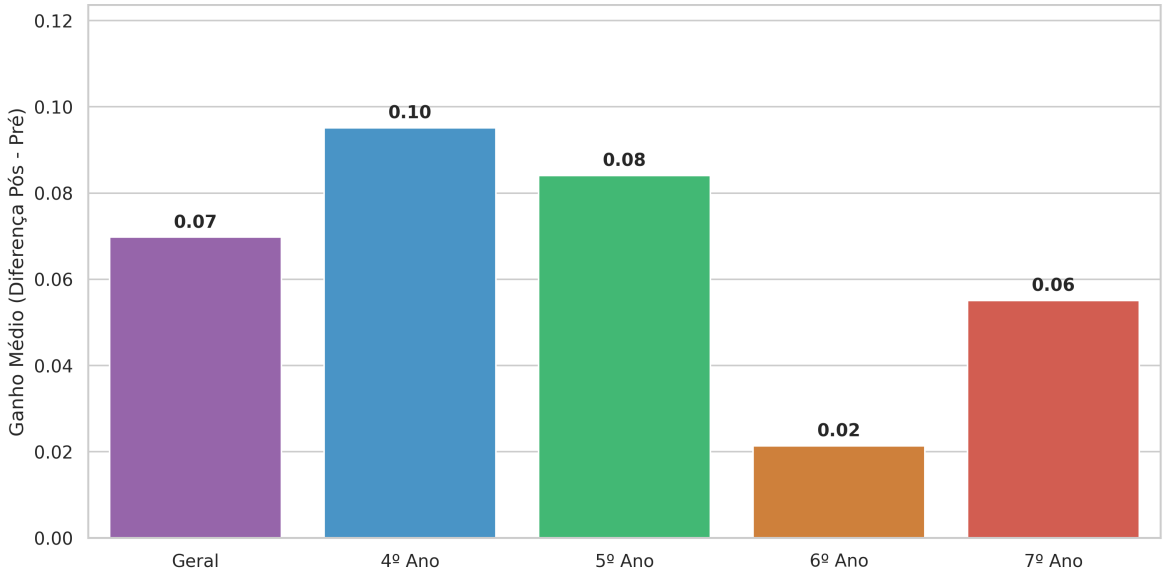
Figura 33 – Melhora média do desempenho pós intervenção.



Fonte: Elaboração própria.

Esse fato se confirma ao observar, de forma individual, cada uma das turmas, nas quais se verifica que, quanto mais novos os estudantes, maior é a melhora média obtida. Como exceção, destaca-se o 6º ano, que apresentou a menor melhora média entre todas as turmas analisadas. A Figura 34 apresenta a relação do ponto médio de melhora para cada turma.

Figura 34 – Melhora média do desempenho por série.

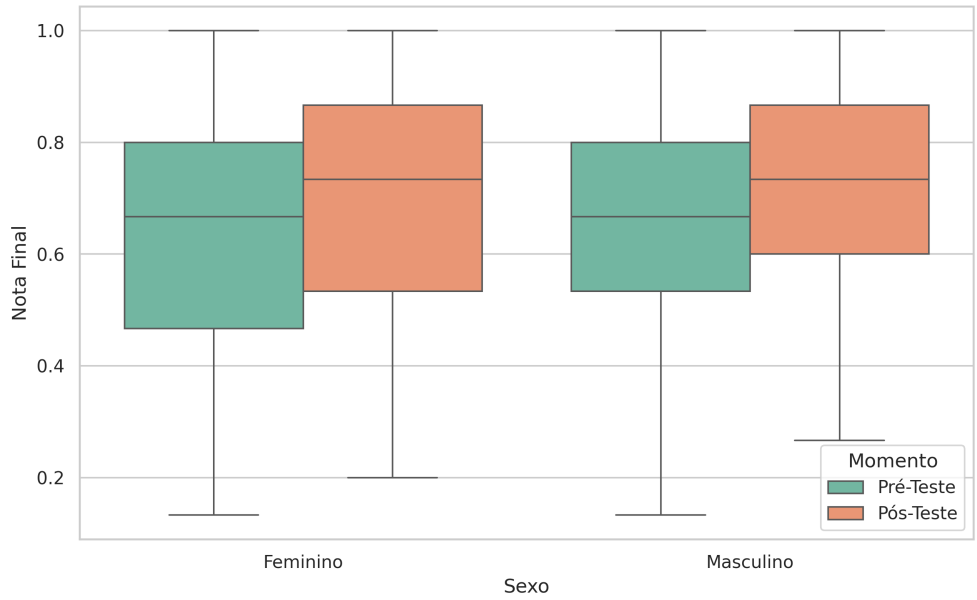


Fonte: Elaboração própria.

Ao realizar a análise baseada no sexo informado dos estudantes, é possível observar que, independentemente do grupo, houve ganho de conhecimento após a intervenção,

conforme apresentado na Figura 35.

Figura 35 – Dispersão das notas: pré *vs* pós por sexo.

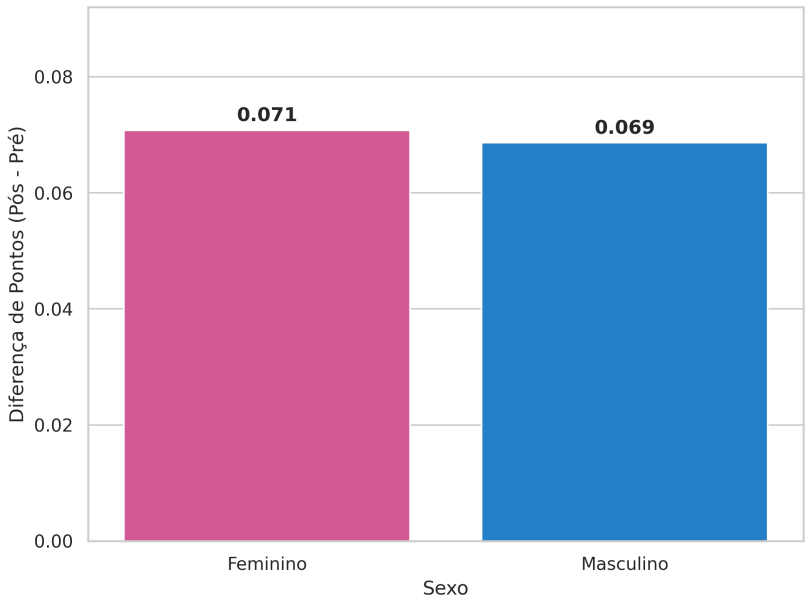


Fonte: Elaboração própria.

Por meio do boxplot, nota-se que a mediana do pós-teste encontra-se acima da mediana do pré-teste, indicando melhora no desempenho dos participantes. Além disso, observa-se que a distribuição das notas no pós-teste permanece relativamente concentrada em torno de valores mais elevados, sugerindo uma tendência de melhora geral entre os estudantes. Adicionalmente, a ausência de *outliers* indica que não houve valores extremos discrepantes nos resultados após a atividade.

Ao analisar o aumento médio, nota-se uma diferença pouco expressiva entre os grupos, com um ganho de desempenho de aproximadamente 7% para ambos. Especificamente, observou-se um ganho de 0,069 para o sexo masculino e de 0,071 para o feminino. Esse resultado reforça o exposto anteriormente, evidenciando que não houve diferenças significativas no desempenho de forma estratificada pelo sexo dos participantes, conforme apresentado na Figura 36.

Figura 36 – Ganho médio de desempenho por sexo.



Fonte: Elaboração própria.

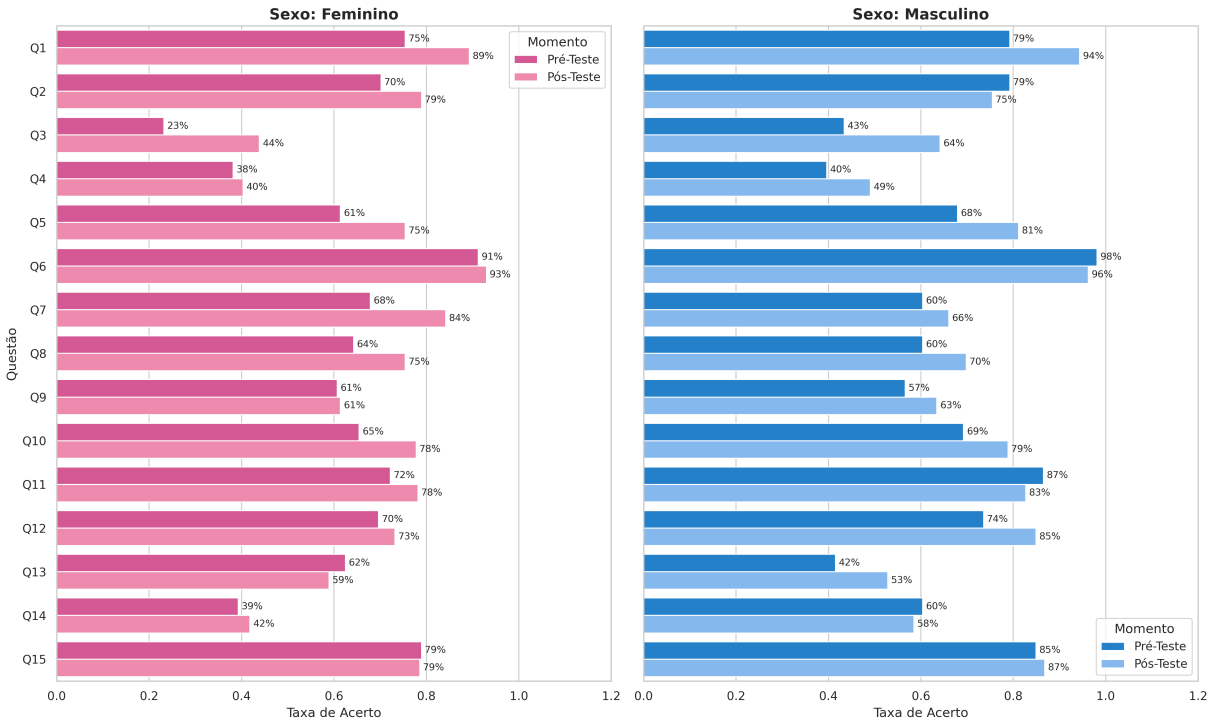
Por fim, ao realizar a análise questão a questão do desempenho no pré e no pós-teste por meio do teste de McNemar, é possível observar melhorias estatisticamente significativas ($p < 0,05$) na questão Q1, com aumentos percentuais de 14% e 15%, respectivamente, para ambos os sexos. Na questão Q3, também foi identificado um ganho expressivo, com aumento de 21% para os dois grupos. Nas questões Q7 e Q8, igualmente, observa-se um ganho relevante para ambos os sexos.

Assim como verificado na análise geral com o teste de McNemar, na questão Q6 observa-se que a taxa de acertos no pré-teste já era elevada, sendo de 91% entre as estudantes do sexo feminino e 98% entre os estudantes do sexo masculino. Dessa forma, havia pouco espaço para aumento no pós-teste, no qual as taxas passaram para 93% e 96%, respectivamente, evidenciando uma discreta redução na taxa de acertos entre os estudantes do sexo masculino.

Observa-se, ainda, que nas questões Q9 e Q15 não houve alteração nos resultados para as estudantes do sexo feminino. Nessas mesmas questões, houve apenas um pequeno aumento entre os estudantes do sexo masculino, especialmente na Q15, indicando pequena variação nos resultados.

Além disso, foi identificado um desempenho inferior para as estudantes do sexo feminino apenas na questão Q13, com uma leve queda de 3%. Já os estudantes do sexo masculino apresentaram reduções nas questões Q2, Q6, Q11 e Q14, indicando um desempenho ligeiramente inferior nesses itens. A Figura 37 apresenta a evolução em cada uma das 15 questões.

Figura 37 – Comparativo de conhecimento aferido por questão e sexo.



Fonte: Elaboração própria.

6.5 Avaliação de Usabilidade e Experiência do Jogador (MEEGA+)

Com o intuito de avaliar a usabilidade e a experiência do jogador, optou-se pela utilização do questionário MEEGA+, amplamente empregado na avaliação de jogos digitais educacionais na área da Computação. O artefato é dividido em duas dimensões principais: usabilidade e experiência do Jogador, totalizando 35 questões, com respostas na escala Likert, na qual os usuários podem atribuir uma nota de 1 a 5 para cada uma das questões, variando de 1 (muito insatisfeito) a 5 (muito satisfeito).

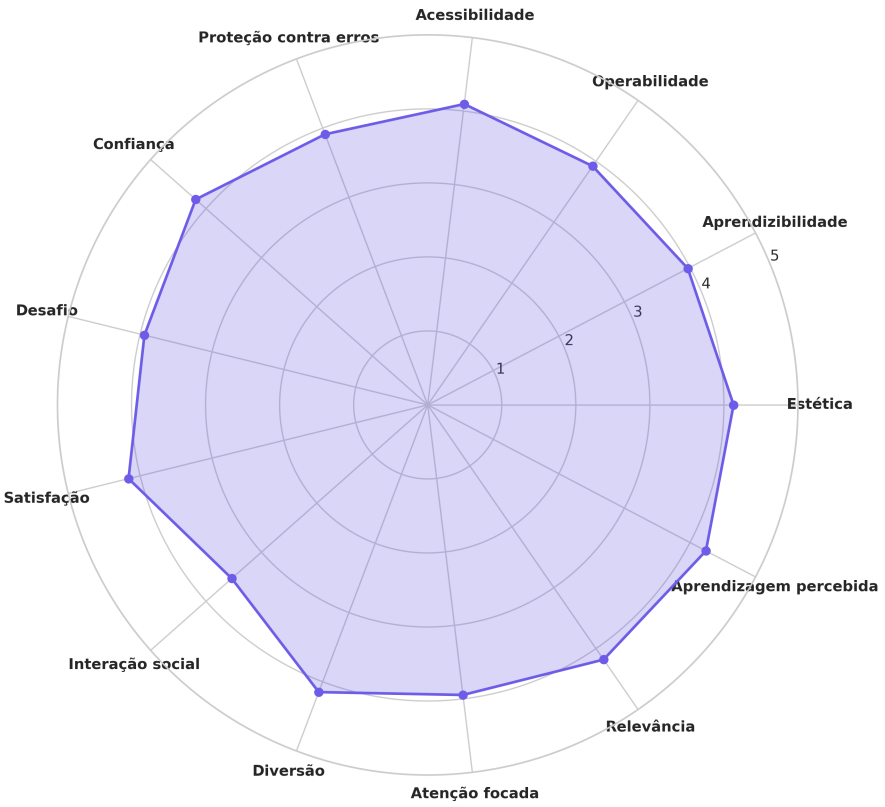
A dimensão de Usabilidade é composta por cinco subdimensões: Estética, Aprendizibilidade, Operabilidade, Acessibilidade e Proteção contra Erros. Já a dimensão de Experiência do Jogador é estruturada em diferentes subdimensões, incluindo: Confiança, Desafio, Satisfação, Interação Social, Diversão, Atenção Focada, Relevância e Aprendizagem Percebida, buscando avaliar de forma abrangente a percepção dos participantes em relação à utilização do jogo.

Ao observar o gráfico de radar na Figura 38 utilizado para analisar todas as esferas do MEEGA+, é possível verificar que dimensões como Diversão, Estética, Aprendizagem Percebida, Confiança e Satisfação foram bem avaliadas pelos estudantes, apresentando médias superiores a 4 pontos na escala Likert.

Por outro lado, também é possível identificar alguns pontos de atenção. A subdimen-

são Interação Social apresentou a menor média entre todas as dimensões avaliadas (3,54), distanciando-se das demais. Além dela, as subdimensões Proteção contra Erros (3,91), Operabilidade (3,92), Desafio (3,94), Atenção Focada (3,95) e Aprendizibilidade (3,97) apresentaram médias ligeiramente inferiores a 4, embora ainda próximas ao valor médio da escala.

Figura 38 – Panorama geral MEEGA+.



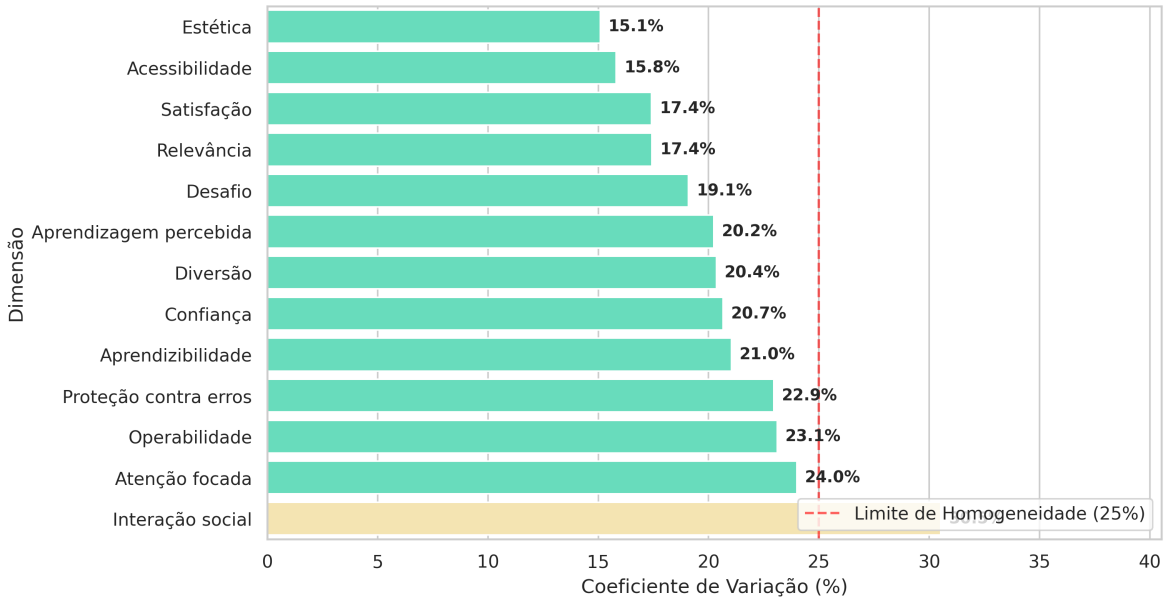
Fonte: Elaboração própria.

Apesar de essas subdimensões terem apresentado médias próximas ao valor médio da escala, seus resultados podem estar relacionados à percepção dos estudantes quanto à facilidade de compreender como jogar e utilizar os comandos, à capacidade do jogo de evitar ou minimizar problemas decorrentes de erros durante a interação, à rapidez com que aprenderam a utilizar suas mecânicas e ao equilíbrio entre o nível de desafio e a manutenção da atenção ao longo da experiência. Esses aspectos podem ter influenciado negativamente a avaliação dessas subdimensões.

Ao analisar o coeficiente de variação (CV), observa-se uma relativa homogeneidade nas respostas dos estudantes em praticamente todas as subdimensões do MEEGA+, com exceção da Interação Social, discutida anteriormente. Esse resultado pode ser explicado pelo fato de o jogo proporcionar uma experiência predominantemente *single player*, na qual a interação entre os participantes não é necessária para a conclusão da atividade.

As dimensões Estética, Acessibilidade, Satisfação e Relevância apresentaram os menores coeficientes de variação (entre 15,1% e 17,4%), indicando elevada concordância entre os estudantes quanto às suas percepções nesses aspectos. As demais dimensões também permaneceram abaixo do limite de homogeneidade de 25%, evidenciando baixa dispersão das respostas e reforçando a consistência das avaliações obtidas por meio do MEEGA+, conforme ilustrado na Figura 39.

Figura 39 – Coeficiente de variação das respostas ao MEEGA+.



Fonte: Elaboração própria.

Antes da realização das análises de correlação e regressão, foram verificados os pressupostos estatísticos dos dados obtidos pelo questionário MEEGA+. O teste de Shapiro-Wilk indicou violação da hipótese de normalidade em todas as esferas avaliadas ($p < 0,05$). Em seguida, o teste de Levene foi aplicado para avaliar a homogeneidade das variâncias, sendo identificada homogeneidade em 12 das 13 subdimensões analisadas e heterocedasticidade apenas na subdimensão Operabilidade ($p < 0,05$). Esses resultados justificaram a utilização do coeficiente de correlação de postos de Spearman nas análises de associação e a estimação dos modelos de regressão com erros-padrão robustos (HC3).

Para aprofundar a análise da variável dependente Aprendizagem Percebida, foi ajustado um modelo de regressão linear múltipla com erros-padrão robustos (HC3). Foram selecionadas as cinco subdimensões que apresentaram coeficiente de variação inferior a 20%, indicando maior homogeneidade nas respostas e maior consenso entre os participantes.

Observa-se que a subdimensão Satisfação apresentou a associação positiva mais pronunciada entre as variáveis investigadas (0,337). Esse resultado indica uma tendência de aumento na aprendizagem percebida à medida que a satisfação dos estudantes com o jogo

se eleva.

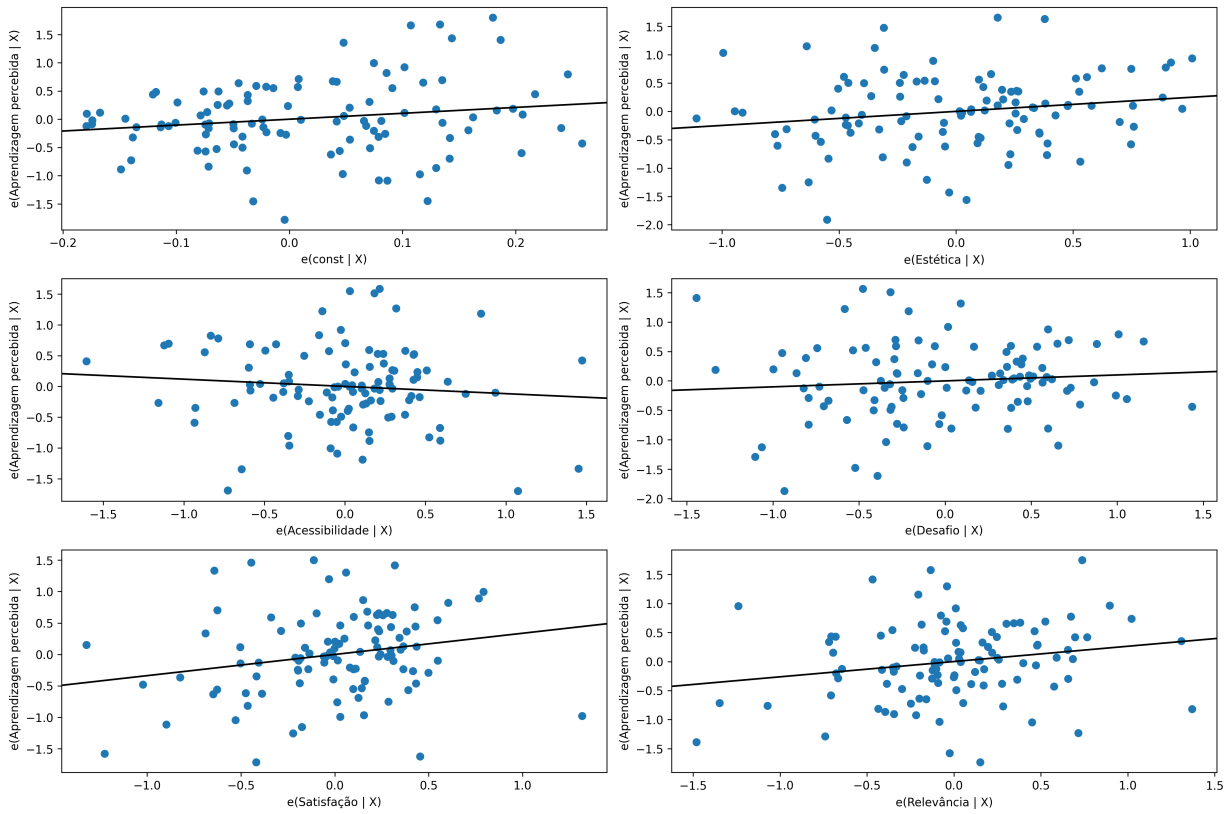
Em seguida, as subdimensões Estética (0,247) e Relevância (0,263) também apresentaram associação positiva com a aprendizagem percebida, embora com menor intensidade. Esses resultados sugerem que aspectos relacionados à relevância da experiência e à qualidade estética do jogo podem ter contribuído para a percepção de aprendizagem.

Por outro lado, a subdimensão Acessibilidade apresentou associação negativa (-0,117), indicando que, no contexto analisado, não se observa uma relação positiva entre acessibilidade e aprendizagem percebida. Esse resultado sugere que, neste modelo, aspectos relacionados à acessibilidade do *software* não se mostraram associados de forma relevante à percepção de aprendizagem dos estudantes.

Dentre as subdimensões analisadas que apresentaram impacto positivo, Desafio demonstrou o menor coeficiente (0,101), indicando baixa contribuição para a variação da aprendizagem percebida neste contexto. Esse resultado pode estar relacionado à percepção dos estudantes sobre o nível de desafio apresentado pelo jogo, dadas suas habilidades e expectativas durante a atividade.

Esses resultados sugerem que a percepção de aprendizagem não está associada de forma uniforme a todas as subdimensões avaliadas, sendo a Satisfação a variável que exerce o maior impacto positivo sobre a percepção de aprendizagem dos participantes. Assim, estudantes que atribuíram maiores níveis de satisfação também tenderam a relatar maior aprendizagem percebida. A relação entre o item Aprendizagem Percebida e as demais variáveis pode ser observada na Figura 40.

Figura 40 – Gráfico de regressão parcial para a variável dependente Aprendizagem Percebida.



Fonte: Elaboração própria.

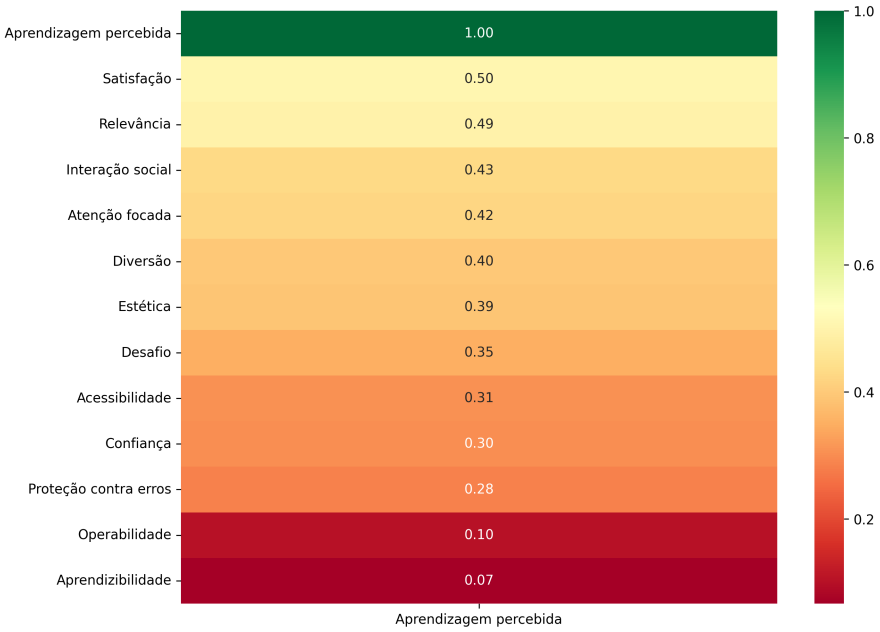
Adicionalmente, ao analisar as demais variáveis do modelo, foi possível observar que as variáveis associadas a aspectos afetivos da experiência, como Satisfação, Relevância e Estética, apresentaram maior contribuição para a percepção de aprendizagem dos estudantes. Notou-se que todas as subdimensões associadas à esfera da Experiência do Jogador apresentaram associações positivas, mesmo que de menor intensidade. Por outro lado, com exceção da variável Estética, as demais subdimensões relacionadas à esfera da Usabilidade, como Operabilidade (-0,127), Acessibilidade (-0.117), Aprendizibilidade (-0,086) e Proteção contra erros (-0,070), não apresentaram influência positiva sobre a aprendizagem percebida.

Esse resultado sugere um padrão de maior associação entre a percepção de aprendizagem e aspectos subjetivos da experiência dos estudantes com o jogo, em comparação a fatores estritamente funcionais da interface. Isso evidencia que, embora a usabilidade seja um pré-requisito fundamental para a interação com o sistema, ela não atua como o principal motor da aprendizagem percebida neste contexto. Em outras palavras, a facilidade de navegação e a ausência de erros funcionais asseguram uma experiência livre de frustrações técnicas, mas não garantem, por si sós, que o jogador absorva o conteúdo proposto com maior eficácia.

Ao analisar o panorama geral por meio da correlação de Spearman, considerando todas

as subdimensões e suas associações com a variável dependente Aprendizagem Percebida, observa-se uma forte relação da Satisfação com o aprendizado dos estudantes, seguida pela Relevância. Complementarmente, como já observado, as variáveis relacionadas à esfera da Usabilidade, como Aprendizibilidade (0,07), Operabilidade (0,10) e Proteção contra Erros (0,28), associadas à correta operação do software, também não apresentaram impacto expressivo na aprendizagem percebida pelos jogadores, conforme ilustrado na Figura 41.

Figura 41 – Força da relação: o que mais impacta a Aprendizagem Percebida?



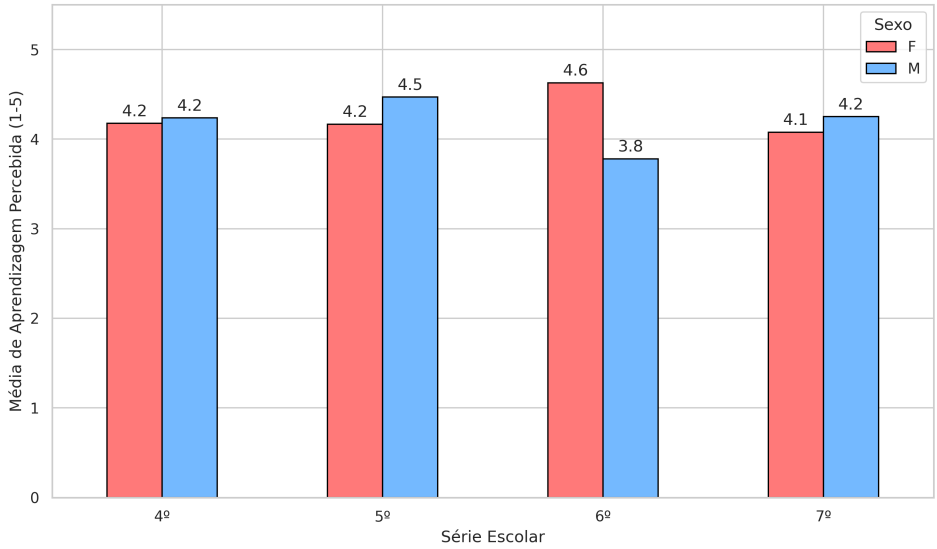
Fonte: Elaboração própria.

Com base no panorama observado, torna-se pertinente verificar se a percepção de aprendizagem se mantém homogênea entre os diferentes perfis de estudantes que compõem a amostra, considerando fatores como sexo e série escolar.

Observou-se uma média geral semelhante entre os sexos (4,25 para o feminino e 4,23 para o masculino). Esses resultados sugerem que, de forma geral, estudantes do sexo feminino e masculino apresentaram percepções semelhantes em relação à subdimensão Aprendizagem Percebida, indicando que a ferramenta proporcionou uma experiência consistente entre esses grupos.

Conforme apresentado na Figura 42, observa-se que os estudantes atribuíram, em sua maioria, notas superiores a 4 para a subdimensão Aprendizagem Percebida em todas as turmas avaliadas. De forma semelhante, ao analisar os resultados por sexo, as médias permaneceram acima de 4 em praticamente todos os grupos, com exceção dos estudantes do 6º ano do sexo masculino, que apresentaram média de 3,8. De modo geral, esses resultados sugerem que fatores individuais, como sexo e série escolar, não estiveram associados a diferenças perceptíveis na percepção de aprendizagem dos participantes, indicando que a experiência proporcionada pelo jogo foi semelhante entre os diferentes perfis analisados.

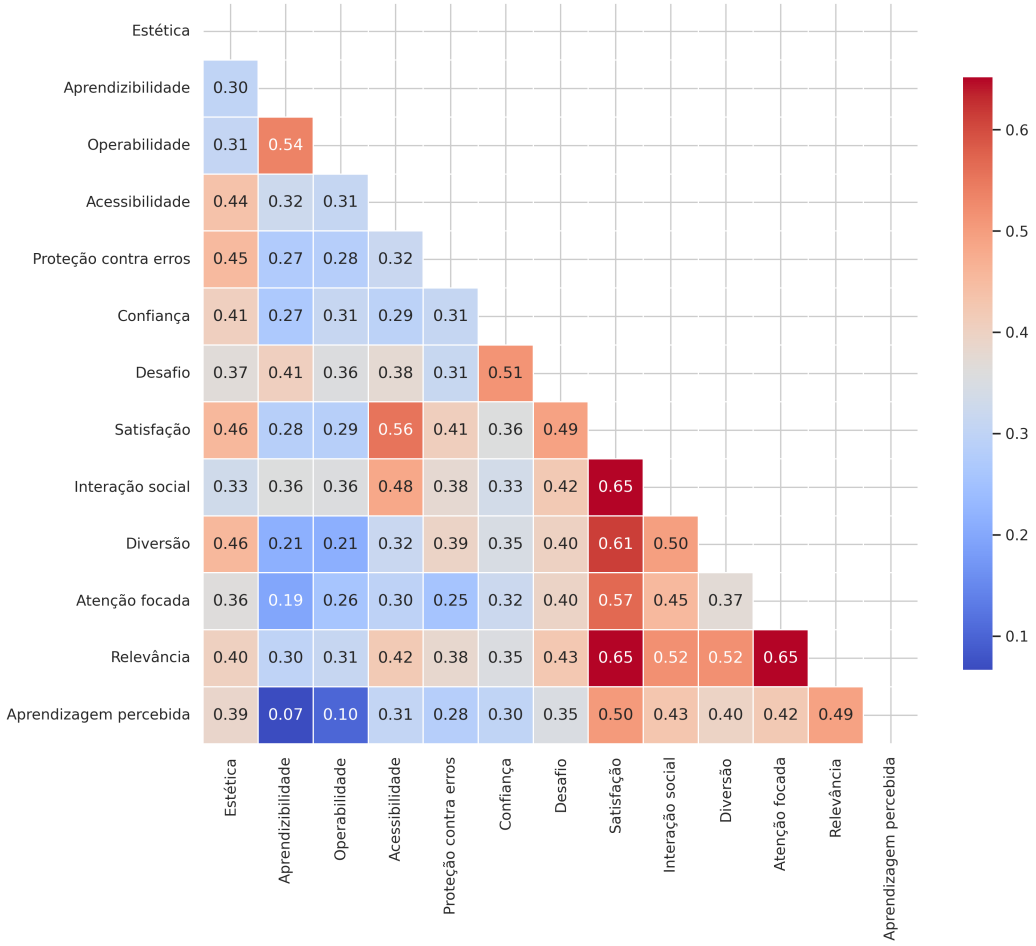
Figura 42 – Média da Aprendizagem Percebida por sexo e série escolar.



Fonte: Elaboração própria.

Por fim, por meio do mapa triangular apresentado na Figura 43, é possível realizar uma análise geral das relações entre todas as esferas do MEEGA+ e como elas se interconectam. Ao analisar a Satisfação dos estudantes com a atividade, observa-se uma forte correlação com a Interação Social (0,65). Esse resultado sugere que, embora o jogo seja predominantemente *single player*, a possibilidade de interação entre os usuários durante a aplicação da atividade, não restrita pelo ambiente, contribuiu para uma experiência mais satisfatória.

Figura 43 – Mapa de inter-relação das dimensões MEEGA+.



Fonte: Elaboração própria.

Além disso, a Satisfação também apresenta forte correlação com a Relevância (0,65), indicando que a percepção de utilidade do conteúdo e sua aplicabilidade futura influenciam diretamente a motivação dos estudantes. Observa-se, ainda, uma forte correlação entre Diversão e Satisfação (0,61), evidenciando que experiências mais agradáveis e envolventes tendem a aumentar o nível de satisfação dos jogadores.

Adicionalmente, observa-se que a Satisfação também apresenta correlação relevante com a Acessibilidade, sugerindo que os estudantes perceberam o jogo como utilizável sem barreiras expressivas. Nesse sentido, a acessibilidade pode ser entendida como um fator facilitador do aprendizado, uma vez que sistemas mais acessíveis tendem a promover maior engajamento. Por outro lado, quando há barreiras de uso, a motivação pode ser reduzida, impactando negativamente a aprendizagem percebida pelos jogadores.

De modo geral, a Satisfação se destaca como uma das variáveis centrais no gráfico de correlações, apresentando conexões fortes com subdimensões como Atenção Focada, Relevância e Aprendizagem Percebida, o que reforça seu papel como elemento-chave na experiência educacional proporcionada pelo jogo.

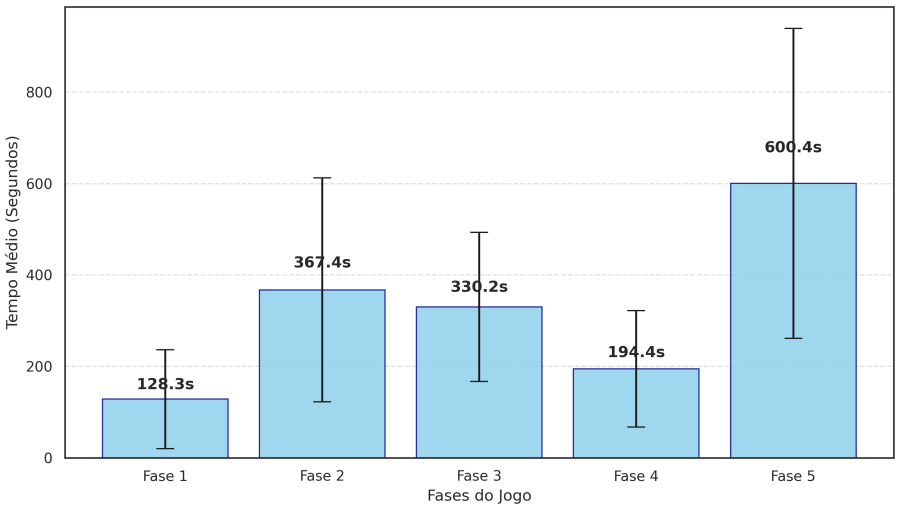
6.6 Análise de Comportamento por meio dos *Logs* da Aplicação

Com o intuito de complementar os dados obtidos nas etapas de pré e pós-teste e do questionário MEEGA+, foram coletados os *logs* do jogo durante a atividade. O objetivo foi verificar se o ganho de conhecimento objetivo e a aprendizagem percebida estão alinhados com o desempenho real dos estudantes durante a interação com a ferramenta.

O teste de Shapiro-Wilk indicou violação da hipótese de normalidade nas métricas extraídas dos *logs* ($p < 0{,}05$). Em seguida, o teste de Levene foi empregado para avaliar a homogeneidade das variâncias entre as métricas de tempo, erros, acertos, abandonos e taxa de conclusão. Os resultados evidenciaram heterocedasticidade entre essas métricas, indicando variabilidade no comportamento dos jogadores durante a interação com o jogo. Apesar disso, a taxa de conclusão apresentou maior proximidade com a homogeneidade ($p = 0{,}0482$). Em razão desses resultados, as análises de associação foram conduzidas por meio do coeficiente de correlação de postos de Spearman.

A análise do tempo médio despendido em cada uma das cinco fases permite inferir o comportamento dos jogadores diante dos desafios propostos. Conforme apresentado na Figura 44, a Fase 1 demandou o menor tempo médio ($128,3s$), o que sugere um esforço reduzido para a sua conclusão, condizente com uma etapa introdutória. Observa-se uma progressão no grau de dificuldade nas fases subsequentes, com uma sutil tendência de declínio na Fase 4. Esse comportamento pode indicar que os jogadores conseguiram assimilar os conceitos pedagógicos de forma mais célere nesta etapa, demonstrando maturidade em relação às mecânicas do jogo.

Figura 44 – Esforço médio por fase com dispersão (desvio padrão).



Fonte: Elaboração própria.

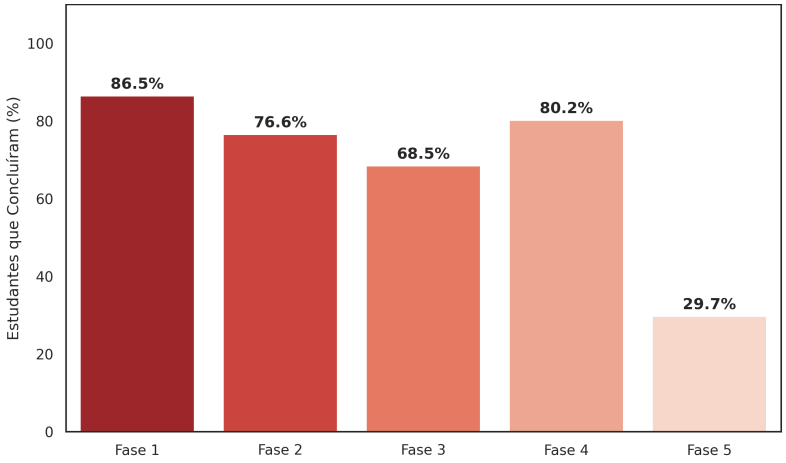
A Fase 5 apresentou o maior tempo médio de execução ($600,4s$), consolidando-se como

o estágio mais desafiador do jogo. Observou-se uma trajetória ascendente no número de tentativas, que partiu de 168 (Fase 1), seguiu com 187 (Fase 2), 205 (Fase 3) e 204 (Fase 4), culminando em 309 tentativas na Fase 5. Apesar da complexidade, os dados de permanência e número de tentativas indicam um forte engajamento, sugerindo que a fase foi capaz de manter o interesse e a persistência dos participantes até a sua conclusão. O elevado desvio padrão observado nesta etapa final também evidencia uma maior heterogeneidade no esforço despendido e nas estratégias adotadas pelos estudantes para superar os desafios propostos.

Complementando as observações iniciais, A Figura 45 mostra a taxa de conclusão de cada uma das cinco fases propostas. A Fase 5 consolidou-se como a etapa de maior dificuldade para os jogadores, apresentando uma taxa de conclusão de apenas 29,7%. Este dado corrobora a análise anterior, indicando que os estudantes enfrentaram desafios para superar as barreiras desta fase.

Além disso, a quinta fase do jogo foi a que apresentou maior exigência de coordenação motora, demandando respostas rápidas e maior precisão na interação com a ferramenta. Esse aspecto pode ter contribuído para o elevado número de tentativas registrado nessa etapa, bem como para a desistência de alguns estudantes, uma vez que o desempenho passou a depender não apenas da compreensão dos conceitos de cibersegurança, mas também de habilidades relacionadas ao tempo de reação e ao controle dos dispositivos de entrada.

Figura 45 – Taxa de conclusão por fase do jogo.



Fonte: Elaboração própria.

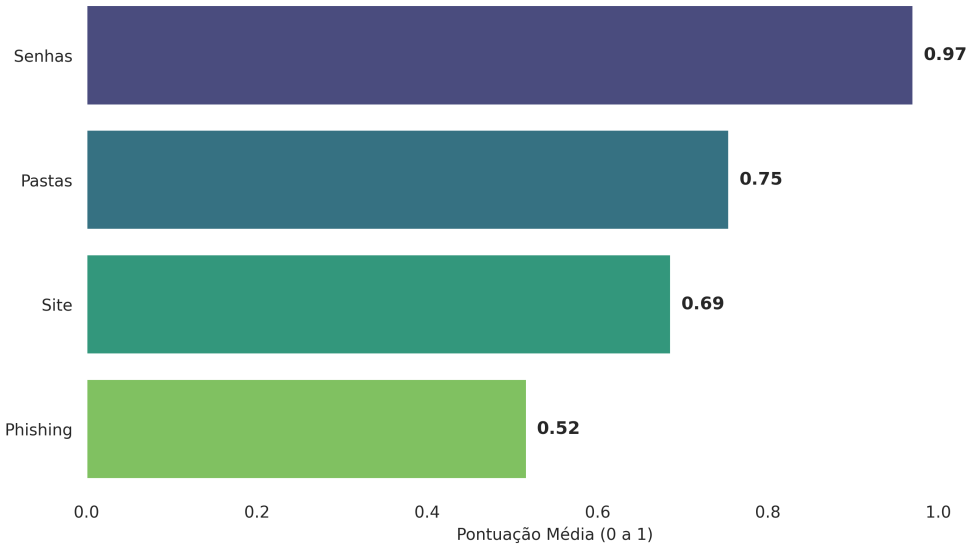
Em contrapartida, as Fases 1 e 4 demonstraram um elevado índice de sucesso, com taxas de conclusão superiores a 80%. Tais resultados indicam que as mecânicas de jogo adotadas nessas etapas foram acessíveis, permitindo que os jogadores interagissem com o conteúdo proposto sem barreiras técnicas expressivas que impedissem seu progresso.

Ainda, as Fases 2 e 3 apresentaram um desempenho intermediário, com taxas de

conclusão acima de 68%, o que evidencia um incremento na dificuldade ao longo do jogo. É importante ressaltar que a conclusão dessas fases reflete, primariamente, a manutenção do engajamento dos estudantes e a eficácia do *design* do jogo em guiar o jogador pelos desafios, criando a base necessária para que a assimilação dos conceitos pedagógicos ocorra de forma estruturada.

Ao analisar a Figura 46, que apresenta a eficácia média dos participantes nas quatro mecânicas principais do jogo, observa-se que os estudantes demonstraram domínio sobre a criação de senhas, alcançando uma pontuação média de 0,97. Isso indica que a maioria absoluta compreendeu e aplicou corretamente os critérios de segurança para essa tarefa.

Figura 46 – Desempenho médio por fase do jogo.



Fonte: Elaboração própria.

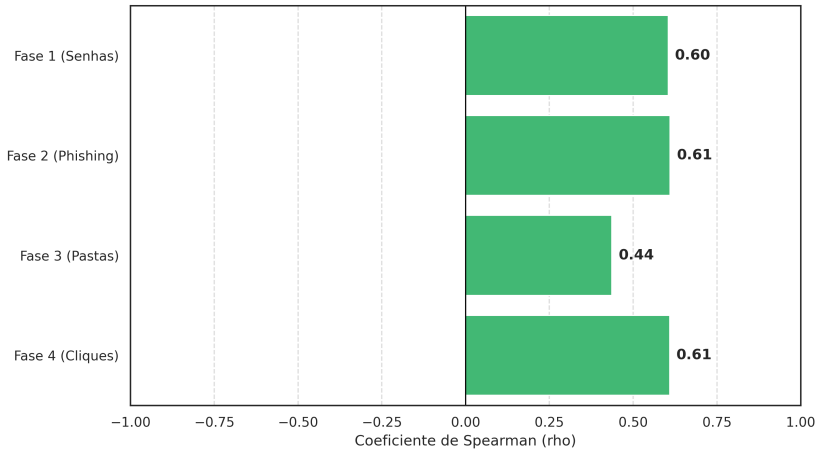
Em contrapartida, a mecânica de *phishing* registrou o desempenho mais baixo entre as categorias analisadas, com média de $0,52$. Essa disparidade sugere uma dificuldade de compreensão dos objetivos pedagógicos desta etapa, o que foi corroborado pelas observações de campo: notou-se que os estudantes mais jovens tendiam a negligenciar a leitura das mensagens, agindo de forma impulsiva. Por fim, as pontuações nas fases de sites maliciosos $(0,69)$ e pastas seguras $(0,75)$ posicionaram-se em uma faixa intermediária, situando-se entre os resultados observados em *phishing* $(0,52)$ e senhas $(0,97)$, evidenciando que os estudantes conseguiram, em sua maioria, identificar elementos maliciosos em interfaces web e distinguir arquivos seguros de ameaças durante a atividade.

Considerando as características estatísticas dos dados, a análise de associação entre o tempo de execução e o desempenho dos estudantes foi realizada por meio da correlação de postos de Spearman. Os resultados revelam um fenômeno central no comportamento dos jogadores: a relação entre o tempo despendido e o desempenho é mais acentuada nas etapas que exigem maior carga cognitiva de leitura e interpretação.

Na Fase 2 (0,61) e na Fase 4 (0,61), onde o estudante deve analisar atentamente e-mails e elementos de sites, a correlação positiva forte confirma que o aumento no tempo de execução está diretamente ligado à melhoria do desempenho. Em outras palavras, o sucesso nessas etapas depende de uma postura reflexiva e da manutenção da atenção.

Por outro lado, esse fenômeno é menos expressivo na Fase 3 (0,44). Sendo esta uma etapa de mecânica mais "frenética" (coleta de pastas) em um jogo de plataforma, a natureza da tarefa altera a dinâmica do esforço: tempos excessivamente longos aqui podem não indicar reflexão, mas sim dificuldades na percepção visual ou na agilidade motora, uma vez que a liberdade de repetir a fase sugere que a eficiência (acerto rápido) é o comportamento esperado para o domínio da mecânica. A correlação de Spearman pode ser visualizada na Figura 47.

Figura 47 – Correlação de Spearman: tempo de execução *vs* performance.



Fonte: Elaboração própria.

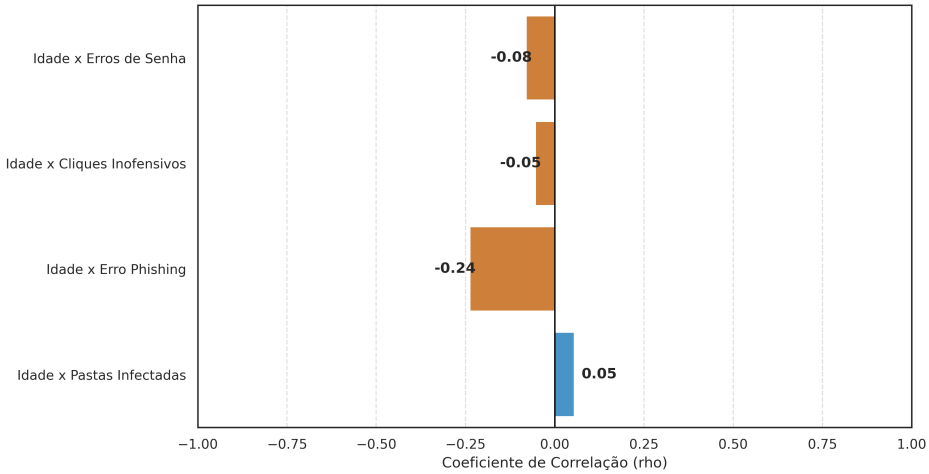
A compreensão dos fatores que influenciam o desempenho pode estar associada tanto às características das tarefas, como sua carga cognitiva e natureza, quanto a características individuais dos participantes. Nesse sentido, torna-se relevante investigar se as variações de desempenho também estão relacionadas a fatores como série escolar, idade e sexo.

A análise da Correlação de Spearman entre a idade e o volume de erros cometidos (Figura 48) revela que a faixa etária não foi um fator determinante para o desempenho na maioria das mecânicas, evidenciando a acessibilidade do jogo.

Entretanto, observa-se uma correlação negativa mais acentuada na mecânica de *phishing* (-0,24). Em termos estatísticos, este índice indica que, conforme a idade aumenta, a tendência de cometer erros nesta fase diminui. Este resultado corrobora as observações qualitativas realizadas durante a aplicação, onde se percebeu que estudantes mais jovens apresentavam maior impulsividade e menor dedicação à leitura dos e-mails propostos. Já nas mecânicas de senhas, cliques em pontos inofensivos do site e pastas infectadas coletadas, os coeficientes próximos de zero indicam que o sucesso nessas tarefas foi inde-

pendente da idade, sugerindo que o *design* pedagógico dessas fases foi compreendido de forma homogénea por diferentes faixas etárias.

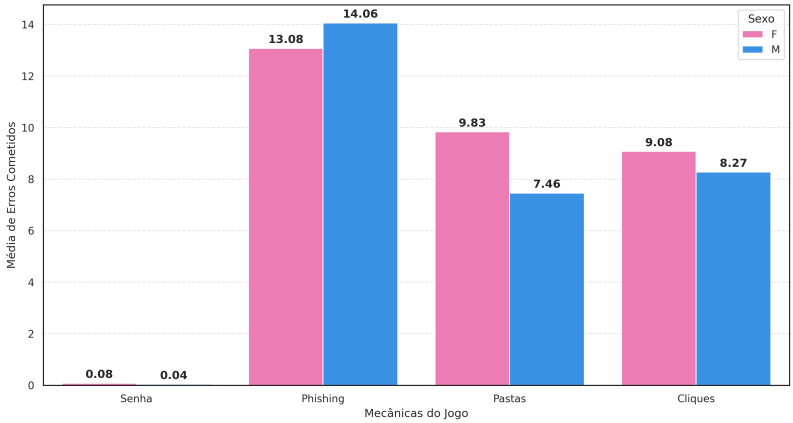
Figura 48 – Influência da idade sobre os erros no jogo (Spearman).



Fonte: Elaboração própria.

Fenômeno semelhante é observado ao comparar o desempenho entre os sexos dos participantes. Conforme ilustrado na Figura 49, nota-se que não houve diferença expressiva entre os grupos, o que pode indicar que o *design* do jogo não beneficia nenhum grupo em específico, permitindo sua utilização por diferentes perfis de usuários. É possível verificar uma média de erros ligeiramente superior entre os estudantes do sexo masculino na fase de *phishing* (14,06 vs. 13,08), enquanto o público feminino apresentou oscilações levemente maiores nas demais fases. Contudo, as margens permanecem muito próximas, reforçando a ideia de que o desempenho global foi equilibrado entre todos os estudantes.

Figura 49 – Comparação de desempenho médio por sexo (análise de erros).

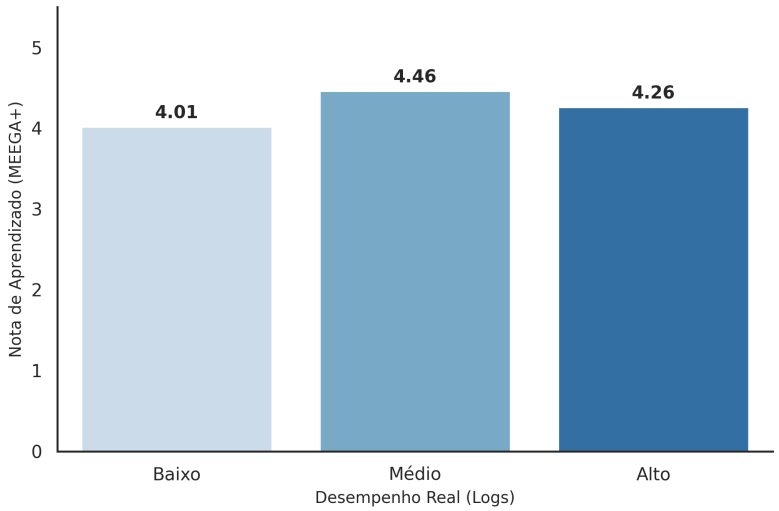


Fonte: Elaboração própria.

Com base nos dados de Aprendizagem Percebida coletados via questionário MEEGA+, foi possível cruzar a percepção subjetiva dos estudantes com seu desempenho real por meio

do cálculo da precisão, definida pela taxa de acertos sobre o volume total de interações (soma de acertos e erros). Conforme apresentado na Figura 50, os estudantes classificados com "Baixo Desempenho" foram os que atribuíram a menor nota à sua própria percepção de ganho de conhecimento, com uma média de 4,01.

Figura 50 – Média de aprendizado por desempenho no jogo.



Fonte: Elaboração própria.

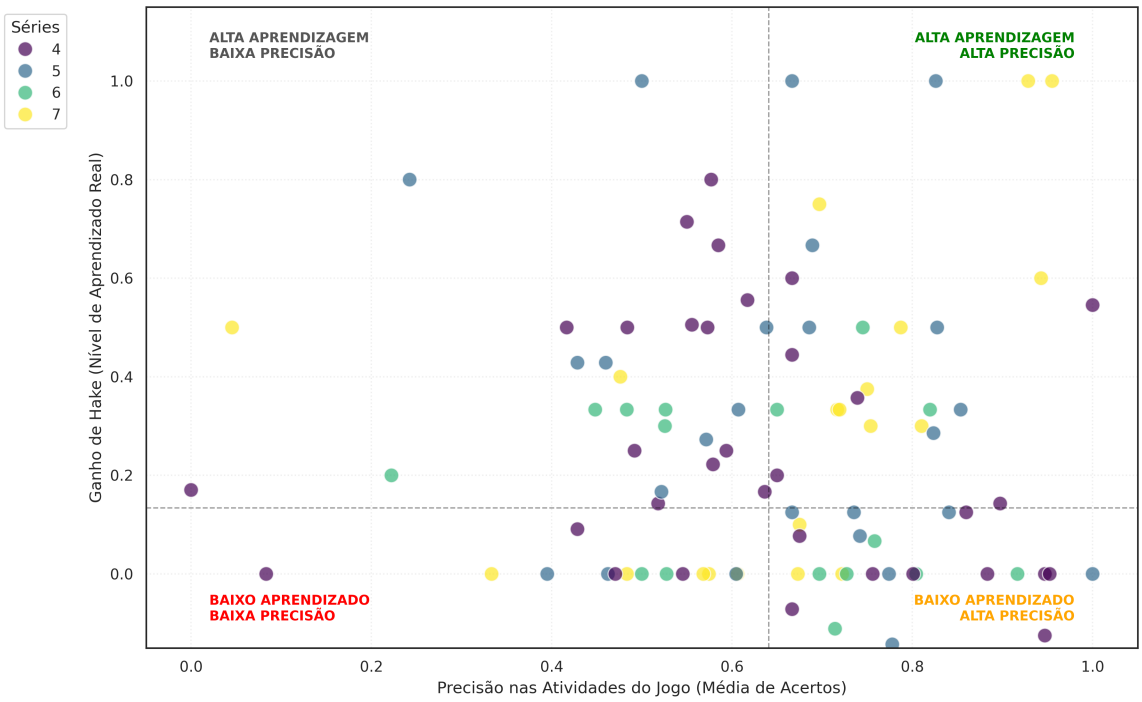
Já os estudantes com desempenho "Médio" foram os que reportaram o maior índice de aprendizado percebido (4,46). Esse resultado sugere que o equilíbrio entre o desafio proposto e a habilidade do jogador favoreceu a sensação de progresso cognitivo. Por fim, o grupo de "Alto Desempenho" atribuiu uma média de 4,26 ao conhecimento percebido. Essa leve queda em relação ao grupo médio pode ser atribuída ao fato de que, para esses estudantes, os desafios lúdicos podem ter sido considerados de baixa complexidade, levando-os a crer que o impacto do jogo em seu estoque de conhecimento prévio não foi tão expressivo quanto para os demais.

Por meio do cruzamento dos *logs* de interação com o desempenho nos testes de conhecimento (Ganho de Hake), a Figura 51 apresenta a relação entre a performance prática e o aprendizado adquirido. Observa-se que a maior concentração de resultados no quadrante de "Baixa Precisão e Baixo Aprendizado" pertence aos estudantes mais jovens (4º ano), o que reforça a hipótese de que a maturidade cognitiva e a fluidez na leitura influenciam o engajamento com o conteúdo textual proposto no jogo.

Em contrapartida, os estudantes do 5º e 7º anos apresentaram picos de "Alta Aprendizagem e Alta Precisão", demonstrando um domínio pleno tanto das mecânicas do jogo quanto dos conceitos avaliados nos testes objetivos. O 6º ano apresentou um comportamento híbrido: uma parte do grupo obteve aprendizado moderado, enquanto a outra se concentrou no quadrante de "Alta Precisão com Baixo Aprendizado". Esse fenômeno sugere que esses estudantes priorizaram a superação dos desafios técnicos em detrimento

da reflexão teórica. Por fim, nota-se uma concentração de estudantes próximos ao eixo zero de aprendizado, mas com alta precisão nas atividades; esse dado indica que o foco desses estudantes recaiu sobre as mecânicas do jogo, tratando a atividade como um desafio técnico, o que pode ter obscurecido a assimilação dos conceitos teóricos pretendidos.

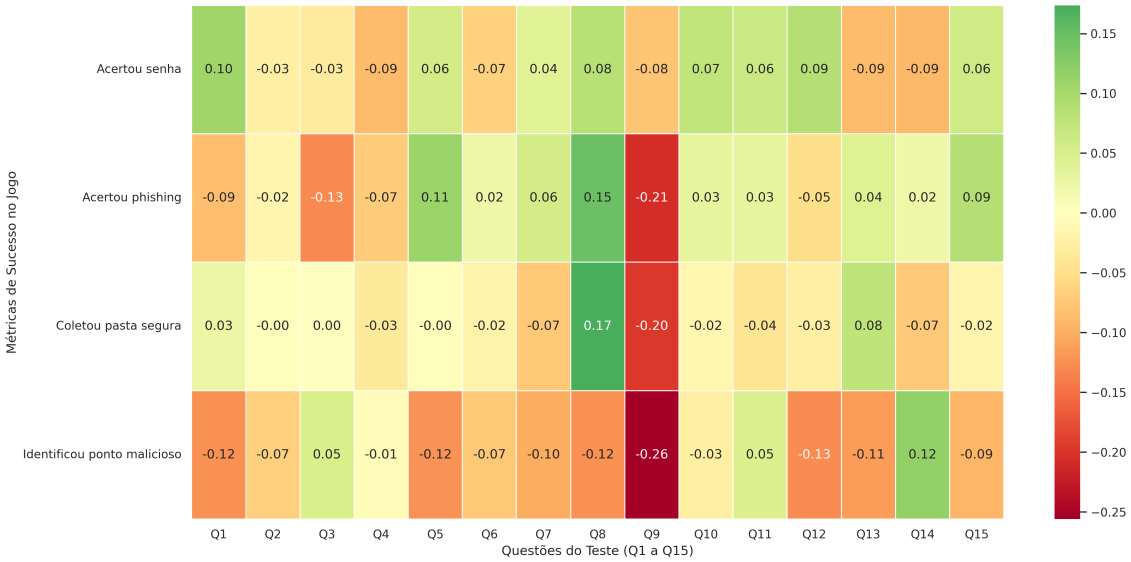
Figura 51 – Matriz de eficácia: performance (*logs*) *vs* aprendizado (Hake).



Fonte: Elaboração própria.

O mapa de calor apresentado na Figura 52 permite visualizar a correlação entre o desempenho no pós-teste e a performance nas fases do jogo. Observa-se que, na primeira fase (senhas), a questão Q1 apresentou uma relação positiva (0,10), enquanto as questões Q2 e Q3 apresentaram uma leve correlação negativa (-0,03 para ambas). Esses resultados sugerem que os estudantes conseguiram transpor o conhecimento sobre senhas de forma relativamente equilibrada entre o ambiente lúdico e o teste objetivo.

Figura 52 – Mapa de calor: acertos no jogo *vs* acertos por pergunta (pós-teste).



Fonte: Elaboração própria.

Por outro lado, nota-se uma correlação negativa entre a Q4 (conceituação de *phishing*) e o desempenho na fase correspondente do jogo (-0,07). Conforme observado na análise do desempenho no pré e pós-teste, a Q4 apresentou a menor evolução entre todas as questões, passando de 38,9% para apenas 44,5%. Somado ao fato de que a média de precisão na fase de *phishing* foi a menor do jogo (0,52), esse coeficiente negativo de -0,07 reforça a hipótese de que parte dos estudantes pode ter superado os desafios dessa fase de forma intuitiva ou por tentativa e erro, sem converter essa experiência em um aprendizado conceitual suficientemente sólido para refletir no desempenho da questão correspondente do pós-teste. Nas demais questões relacionadas ao tema (Q5, Q6 e Q7), as correlações foram positivas.

Para a temática de pastas de arquivos, que compreende as questões Q8 e Q9, observa-se um comportamento heterogêneo: uma correlação positiva na Q8 (0,17) e negativa na Q9 (-0,20). Essa última representa a correlação negativa mais acentuada entre as questões analisadas. Na Q9, os estudantes eram convidados a indicar como evitar a obtenção de arquivos maliciosos, o que pode indicar que, embora tenham obtido bom desempenho na fase correspondente do jogo, nem todos conseguiram consolidar esse conhecimento em nível conceitual. Dessa forma, o sucesso na atividade lúdica nem sempre se refletiu no acerto da questão teórica. Já a temática de sites maliciosos (Q10 e Q11) apresentou correlações próximas de zero, indicando baixa associação entre o desempenho no jogo e os acertos no pós-teste para esse conteúdo.

Por fim, na última questão (Q15), os estudantes foram convidados a realizar uma síntese de todo o conteúdo apresentado pelo jogo. A partir do mapa, é possível observar uma relação heterogênea entre as variáveis analisadas. Esse resultado pode ser explicado pelo fato de a questão abordar a cibersegurança de forma mais ampla, exigindo a integração

de diferentes conceitos trabalhados ao longo da experiência. Nessa situação, além dos conhecimentos construídos durante o jogo, é provável que os estudantes também tenham recorrido aos seus conhecimentos prévios para formular suas respostas. Esse desempenho reflete a complexidade da transferência da aprendizagem para contextos mais abrangentes, uma vez que a síntese dos conteúdos exige um nível de processamento cognitivo mais elevado do que o requerido nas questões específicas das etapas anteriores.

6.7 Análise de Comportamento por meio da Observação Direta

A análise do comportamento dos estudantes foi realizada por meio de observação direta, metodologia que consiste em observar, ouvir e examinar o objeto de estudo de forma reflexiva e descritiva, exigindo contato direto do pesquisador com o objeto (ANA; LEMOS, 2018). Esta abordagem teve como objetivo corroborar com os resultados apresentados anteriormente, permitindo uma visão abrangente sobre o desempenho e o comportamento dos estudantes. Os dados aqui discutidos, baseados em medições e registros coletados durante a atividade, possibilitaram uma compreensão aprofundada da investigação, auxiliando na identificação de manifestações verbais e argumentos que reforçam os achados obtidos, servindo, ainda, como subsídio para pesquisas futuras.

6.7.1 Influência dos Elementos Visuais e Narrativos

Durante a atividade, observou-se que a afinidade por determinados personagens influenciou a escolha das fases, levando os estudantes a priorizar etapas associadas a suas preferências, mesmo quando orientados a seguir uma sequência pré-definida. Esse comportamento, que pode ter contribuído para uma maior permanência e dedicação nessas atividades, estendeu-se à escolha de fases consideradas mais complexas, motivada pela atração por desafios ou por elementos visuais mais estimulantes.

Elementos visuais e interativos, como animações em menus, efeitos de brilho e as transições ao passar o mouse, mostraram-se fundamentais para captar a atenção e aumentar o engajamento inicial, sobretudo entre os estudantes mais novos. Além disso, notou-se o interesse dos participantes em ativar o som do jogo para ampliar a imersão, o que sugere que trilhas musicais e efeitos sonoros possuem um papel relevante na motivação durante a experiência gamificada, ainda que essa funcionalidade não tenha sido habilitada por restrições do laboratório de informática utilizado.

Por fim, o comportamento exploratório dos estudantes foi evidenciado pela tentativa de acessar áreas restritas do sistema, como a seção do professor, demonstrando interesse em funcionalidades adicionais além do escopo inicial. Paralelamente, a utilização do instrumento MEEGA+ com apelo visual, mediante o uso de *emojis*, despertou curiosidade

e vontade de interação lúdica com o material, confirmando a relevância desses elementos no contexto da avaliação.

6.7.2 Desafios, Progressão e Motivação

Na fase final, projetada como a mais desafiadora, observou-se um alto nível de dificuldade e momentos de frustração. Ainda assim, muitos estudantes persistiram na tentativa de conclusão, retornando posteriormente mesmo após explorar outras fases. Esse comportamento reforça a importância de um balanceamento adequado da dificuldade e da oferta de diferentes níveis (fácil, médio e difícil) para atender a perfis variados de jogadores.

Além disso, o bloqueio de uma fase específica, referente ao questionário aplicado em formato impresso, resultou em maior engajamento dos estudantes, que demonstraram motivação para concluir as etapas anteriores para desbloquear o conteúdo, mesmo diante da impossibilidade de acesso naquele momento. Esse comportamento evidencia o potencial de mecânicas como progressão e desbloqueio de conteúdo para aumentar a motivação.

6.7.3 Interação Social e Colaboração

Mesmo com a orientação para a realização da atividade de forma individual, observaram-se ações relacionadas ao comportamento colaborativo, com estudantes auxiliando colegas na resolução de desafios. Isso indica o potencial do jogo para promover interação social, mesmo sendo projetado como uma experiência *single player*.

Complementarmente, observou-se uma evolução progressiva no desempenho em fases que exigiam leitura. Inicialmente, muitos estudantes ignoravam os textos e solicitavam ajuda; no entanto, nas fases seguintes, que exigiam habilidades semelhantes, houve uma redução dos pedidos de auxílio, possivelmente associada à familiarização com a dinâmica do jogo. Esse período também revelou um maior envolvimento de alunas em fases que exigiam leitura e análise, promovendo a colaboração ativa entre os colegas. Além disso, respostas abertas indicaram o interesse dos estudantes na ampliação do uso de jogos digitais no ambiente escolar, reforçando o potencial da abordagem gamificada.

Os estudantes também demonstraram forte interesse em saber quando o jogo estaria disponível para acesso online, de modo que pudessem utilizá-lo fora do horário escolar. Este comportamento demonstra que o jogo conseguiu despertar o interesse dos participantes. *Logs* indicaram que alguns estudantes acessaram o jogo fora do ambiente formal da atividade, sugerindo interesse contínuo e engajamento que ultrapassa o contexto escolar.

6.7.4 Diferenças entre Faixas Etárias

Foram identificadas diferenças relevantes no comportamento e no desempenho entre as turmas participantes do estudo. Essas variações se manifestaram em aspectos como nível de autonomia, compreensão dos conteúdos e engajamento com a atividade.

4º e 5º Anos

- ❏ Os estudantes dessas turmas apresentaram menor autonomia, especialmente no 4º ano, com necessidade de maior intervenção para a compreensão das atividades.
- ❏ Foram observadas dificuldades de leitura e interpretação, além de desafios na compreensão de termos técnicos e até mesmo no vocabulário da língua portuguesa.
- ❏ Foi identificado um alto nível de dispersão e respostas rápidas, indicando uma possível superficialidade na execução das tarefas.

6º e 7º Anos

- ❏ Os estudantes dessas turmas demonstraram maior autonomia, sendo capazes de compreender e executar as atividades com pouca intervenção.
- ❏ Apresentaram maior familiaridade com termos tecnológicos e conceitos básicos de cibersegurança, embora ainda houvesse dificuldade com conteúdos mais específicos, como *phishing*.
- ❏ Apesar da maior autonomia, também foi observada dispersão em alguns momentos, porém acompanhada de maior concentração e rapidez na conclusão das atividades.

As diferenças observadas entre as faixas etárias podem estar relacionadas ao estágio de desenvolvimento das habilidades esperadas para cada etapa da educação básica. A BNCC reconhece que os estudantes dos anos iniciais apresentam características distintas em relação aos anos finais, recomendando que as atividades sejam adequadas à faixa etária e ao nível de desenvolvimento dos alunos, especialmente no que se refere à leitura, à interpretação de informações e à compreensão de conceitos mais abstratos. Destaca-se também o papel do docente como mediador do processo de aprendizagem, oferecendo o suporte necessário para favorecer o desenvolvimento dessas competências. Apesar disso, todos os grupos conseguiram participar da experiência proposta, indicando que, embora a intervenção pedagógica tenha sido mais intensa nos anos iniciais, ela não comprometeu a participação nem o desenvolvimento das atividades.

6.7.5 Dificuldades de Compreensão e Leitura

Durante a atividade, conforme já observado na análise por faixa etária, foram identificadas dificuldades na compreensão de termos técnicos comuns e relacionados à cibersegurança, especialmente entre os estudantes mais novos. Termos como *backup*, *phishing*, *link*, nuvem e *streaming*, bem como formatos como *Portable Document Format* (PDF), MP3 e MP4, exigiram maior mediação para uma compreensão adequada.

Além disso, palavras menos frequentes no cotidiano, como “malicioso”, “caracteres especiais”, *“feedback”* e “anexo”, também apresentaram desafios, evidenciando a necessidade de adaptação do conteúdo ao nível de letramento dos estudantes. Em alguns casos, foi necessária a intervenção dos pesquisadores para auxiliar os participantes na compreensão dos termos e possibilitar a continuidade das atividades.

6.7.6 Familiaridade Tecnológica dos Estudantes

De modo geral, os estudantes apresentaram boa desenvoltura técnica, demonstrando facilidade na manipulação dos controles e mecânicas do jogo. Eventuais dificuldades observadas restringiram-se à compreensão das regras e dos objetivos das fases, indicando que o desafio residia na lógica das atividades, e não na operação da interface propriamente dita.

Uma parcela dos participantes, especialmente do sexo masculino, apresentou uma maior fluência com padrões de controle comuns em jogos eletrônicos, como a utilização das teclas WASD para movimentação de personagens, evidenciando um repertório prévio de contato com jogos digitais.

Adicionalmente, verificaram-se comportamentos inesperados, como o uso de ferramentas de inspeção do navegador pelos estudantes para modificar aspectos visuais da interface. Ainda que não previsto no planejamento, esse interesse sinaliza uma curiosidade pela compreensão dos mecanismos técnicos da aplicação, demonstrando que o interesse dos participantes não se limitou ao uso padrão da ferramenta.

6.7.7 Questões de Acessibilidade e Neurodiversidade

As observações apresentadas nesta seção têm caráter exploratório. Não foi realizado levantamento sistemático do número de participantes neurodivergentes nem análise estratificada por diagnóstico. As informações disponíveis decorreram do acompanhamento realizado pela instituição e das observações registradas durante a intervenção. Portanto, os comportamentos descritos não devem ser generalizados a estudantes com TEA ou TDAH.

Estudantes com Transtorno do Espectro Autista (TEA) e Transtorno do Déficit de Atenção e Hiperatividade (TDAH) apresentaram desafios adicionais durante a interação com o jogo, especialmente em situações que exigiam rápida tomada de decisão, leitura de instruções e repetição de tentativas após falhas sucessivas. Em alguns casos, a exposição a *feedback* negativo, associada à dificuldade de concluir determinadas fases, contribuiu para episódios de sobrecarga emocional. Essas situações foram percebidas por meio de manifestações como choro, aumento da agitação, recusa em continuar a atividade e, em casos mais intensos, a necessidade de afastamento temporário do ambiente de aplicação.

É importante ressaltar que todos os estudantes nessas condições estavam acompanhados de um profissional de apoio.

Observou-se, ainda, que a pressão por desempenho e a ausência de mecanismos adaptativos podem ter intensificado essas reações em parte dos participantes. Embora não predominantes, tais situações evidenciam a importância de incorporar aspectos de acessibilidade e neurodiversidade ao desenvolvimento de jogos digitais educacionais, por meio de estratégias como níveis graduais de dificuldade e *feedbacks* mais encorajadores.

6.7.8 Limitações de *Design* Identificadas

No decorrer da atividade, foram identificadas algumas limitações relacionadas ao *design* do jogo, especialmente no que se refere à clareza das interfaces e à comunicação dos objetivos em determinadas fases. Na fase de *phishing*, por exemplo, alguns estudantes demonstraram dificuldade em compreender a quantidade de elementos que deveriam ser identificados, devido à ausência de indicadores de progresso. Essa limitação gerou dúvidas frequentes sobre a conclusão da atividade.

Além disso, em fases mais difíceis, observou-se frustração por parte dos estudantes. Mensagens de *feedback* negativo, como “você perdeu” e “tente novamente”, contribuíram para momentos de desmotivação. Em contrapartida, mensagens positivas, como “parabéns", apresentaram impacto favorável no engajamento dos participantes. Esse comportamento reforça a importância do *design* de *feedback* em sistemas educacionais, evidenciando a necessidade de abordagens mais motivadoras e menos punitivas.

Por fim, observou-se que alguns estudantes apresentaram dificuldades adicionais em fases que exigiam maior coordenação motora, especialmente na primeira, terceira e quinta fases do jogo, nas quais era necessário realizar movimentos precisos e responder rapidamente aos estímulos apresentados. Nessas situações, o desempenho dos participantes pode ter sido influenciado não apenas pela compreensão dos conceitos de cibersegurança, mas também por habilidades relacionadas à coordenação motora, ao tempo de reação e ao controle dos dispositivos de entrada. Em alguns casos, esses fatores podem ter dificultado a conclusão das atividades e até mesmo contribuído para a desistência da fase. Dessa forma, esse aspecto deve ser considerado durante o desenvolvimento de jogos digitais educacionais, buscando um melhor equilíbrio entre as demandas cognitivas e motoras das atividades, de modo que as exigências relacionadas à interação não se sobreponham aos objetivos de aprendizagem propostos.

6.7.9 Síntese da Observação Direta

De modo geral, a análise por observação direta permitiu compreender, de forma qualitativa, a interação dos estudantes com a ferramenta e os fatores que influenciaram sua experiência durante a atividade. As evidências indicam que elementos como personagens,

desafios progressivos, interfaces intuitivas e narrativas bem estruturadas contribuíram para o engajamento e a motivação dos participantes.

Por outro lado, foram identificadas limitações técnicas relacionadas à compreensão de termos específicos, ao *design* de algumas fases e à necessidade de um melhor balanceamento da dificuldade. Paralelamente, observou-se que aspectos de acessibilidade e inclusão devem ser considerados desde a concepção do jogo, uma vez que estudantes com necessidades específicas, como TDAH e TEA, apresentaram demandas particulares de acompanhamento. Adicionalmente, a clareza na comunicação dos objetivos e a implementação de sistemas de *feedback* menos punitivos mostraram-se pontos essenciais a serem aprimorados para otimizar a experiência do usuário.

As diferenças observadas entre as turmas reforçam a influência de fatores como idade, nível de letramento e familiaridade com tecnologias digitais na forma como os estudantes interagem com jogos educacionais.

Por fim, os resultados obtidos por meio da observação direta complementam as análises quantitativas apresentadas nas seções anteriores, contribuindo para uma compreensão mais abrangente do impacto da ferramenta no processo de aprendizagem.

6.8 Ameaças à Validade

Dadas as características deste estudo, ele está sujeito a diferentes ameaças à validade. Nesta seção, são apresentadas as principais ameaças à validade interna e à validade externa, bem como as limitações relacionadas aos instrumentos utilizados para avaliar o conhecimento, o desempenho, a usabilidade e a experiência dos participantes durante a interação com o jogo.

6.8.1 Validade dos Instrumentos de Avaliação

Uma das principais ameaças à validade deste estudo está relacionada à possibilidade de os estudantes memorizarem as questões apresentadas nos testes de conhecimento (pré e pós-teste), o que poderia influenciar o desempenho observado na avaliação final. Entretanto, os instrumentos utilizados foram elaborados com o objetivo de avaliar o raciocínio e a compreensão dos conceitos de cibersegurança, e não apenas a memorização de termos específicos. Dessa forma, buscou-se analisar mudanças na compreensão dos participantes em relação aos conteúdos abordados.

Outra medida adotada para mitigar essa ameaça consistiu no controle rigoroso das condições experimentais. Durante toda a aplicação do estudo, foi proibida a utilização de dispositivos móveis e o acesso à internet, impedindo consultas a fontes externas que pudessem interferir nos resultados obtidos.

Outra ameaça refere-se à possibilidade de alguns estudantes já possuírem conhecimentos prévios sobre os temas abordados. Para minimizar esse efeito, foi aplicado um pré-teste

antes da interação com o jogo, permitindo identificar o nível inicial de conhecimento dos participantes e utilizá-lo como referência para as análises posteriores.

Além disso, diferenças entre as turmas, como nível de escolaridade e letramento digital, poderiam influenciar o desempenho dos participantes. Para reduzir essa ameaça, todas as turmas participaram do estudo seguindo o mesmo protocolo experimental, utilizando os mesmos instrumentos e sob as mesmas condições de aplicação. Adicionalmente, foram realizadas análises considerando fatores como faixa etária, sexo e escolaridade, buscando verificar possíveis influências dessas variáveis sobre os resultados.

A avaliação baseada no método MEEGA+ também apresenta limitações decorrentes da subjetividade inerente aos questionários de percepção. As respostas podem ser influenciadas por fatores individuais, como simpatia pela atividade ou interpretações pessoais dos itens avaliados. Para minimizar esse efeito, garantiu-se o anonimato dos participantes e informou-se que as respostas não teriam qualquer influência sobre seu desempenho escolar ou avaliação acadêmica.

Outra ameaça está relacionada à compreensão do instrumento por estudantes mais jovens, que poderiam apresentar dificuldades na interpretação de questões mais complexas. Para reduzir esse risco, os pesquisadores forneceram orientações durante o preenchimento dos questionários, esclarecendo dúvidas relacionadas à interpretação das perguntas, sem interferir nas respostas fornecidas.

Também foi considerada a possibilidade de inconsistências nos registros (*logs*) do jogo, as quais poderiam comprometer métricas como tempo de interação ou quantidade de ações realizadas. Como estratégia de mitigação, foram identificados e removidos registros contendo valores inconsistentes ou considerados *outliers*, reduzindo possíveis distorções nas análises.

Por fim, a observação direta dos participantes pode provocar alterações comportamentais decorrentes da percepção de estarem sendo observados. Para minimizar esse efeito, os pesquisadores mantiveram uma postura neutra durante toda a aplicação, evitando interferências na interação dos estudantes com o jogo. Além disso, os dados provenientes da observação direta foram utilizados apenas como evidências complementares às demais fontes de coleta de dados, reduzindo possíveis vieses decorrentes da interpretação dos observadores.

6.8.2 Validade Interna

Entre as ameaças à validade interna, destaca-se a possibilidade de os participantes adquirirem conhecimentos sobre os conteúdos de cibersegurança por meio de fontes externas durante o período do estudo, o que poderia influenciar os resultados dos testes. Para minimizar essa ameaça, a pesquisa foi conduzida em um curto intervalo de tempo e concentrada na interação direta com a ferramenta, reduzindo a probabilidade de interferências externas.

Outra possível ameaça refere-se à ocorrência de eventos externos, como aulas de reforço ou discussões sobre os conteúdos durante o período experimental, que poderiam influenciar o desempenho dos participantes. Para reduzir esse risco, todas as atividades foram conduzidas em ambiente controlado e monitorado, buscando garantir que o principal estímulo educacional fosse a utilização do jogo proposto.

6.8.3 Validade Externa

Quanto à validade externa, uma limitação do estudo está relacionada ao fato de a pesquisa ter sido realizada em uma única instituição de ensino, inserida em um contexto educacional específico. Dessa forma, reconhece-se que os resultados obtidos não podem ser generalizados para toda a população de estudantes brasileiros. O objetivo desta pesquisa consiste em fornecer evidências científicas sobre a aplicação da proposta em contextos educacionais semelhantes.

Outra ameaça refere-se ao ambiente de aplicação da pesquisa. Embora o jogo tenha sido avaliado em laboratório e em sala de aula, seu desempenho e a interação dos usuários podem apresentar comportamentos distintos em outros contextos de utilização, como no ambiente domiciliar. Como forma de reduzir essa limitação, o estudo foi conduzido em condições que reproduzem o cenário real de uso pedagógico da ferramenta, aproximando a avaliação das situações previstas para sua utilização.

Capítulo 7

Conclusão

Esta pesquisa teve como objetivo promover o aprendizado de cibersegurança entre estudantes do ensino básico, por meio do desenvolvimento e da avaliação de um jogo digital educacional concebido para estimular, de forma lúdica e acessível, a compreensão e a aplicação de práticas seguras no ambiente virtual. Para alcançar esse objetivo, foi conduzido um estudo empírico que permitiu avaliar tanto a aprendizagem dos estudantes quanto aspectos de usabilidade e de experiência de uso da ferramenta. Para isso, foram formuladas duas questões de pesquisa, as quais guiaram a investigação.

Na RQ1, observou-se melhora estatisticamente significativa entre os escores do pré e do pós-teste, com tamanho de efeito moderado, embora o ganho normalizado de Hake tenha sido classificado como baixo. Considerando a ausência de grupo de controle e a reaplicação do mesmo instrumento, os resultados devem ser interpretados como uma mudança associada à intervenção, e não como evidência causal isolada da eficácia do jogo. Em relação à RQ1.1, as análises realizadas não identificaram diferenças significativas associadas ao sexo dos participantes, enquanto a idade e a série apresentaram algumas variações descritivas em atividades específicas. Esses resultados não permitem concluir pela ausência de influência desses fatores nem comprovar a equidade da ferramenta.

Na RQ2, os *logs* mostraram diferenças no tempo de permanência, no número de tentativas e na conclusão das fases. Esses indicadores, quando triangulados com observações diretas e avaliações positivas sobre as dimensões do MEEGA+, fornecem indícios de persistência e de envolvimento. Entretanto, isoladamente, um tempo maior e um número maior de tentativas também podem indicar dificuldade de compreensão ou de interação.

Além disso, foi possível discutir aspectos relacionados à motivação dos participantes com base nas métricas obtidas pelo instrumento MEEGA+, especialmente aquelas referentes à Satisfação, Confiança e Relevância, que receberam avaliações positivas por parte dos estudantes. Destaca-se, ainda, a forte relação entre a satisfação dos usuários e a aprendizagem percebida, indicando que esses fatores são fundamentais para a jornada de aprendizagem dos estudantes.

A proposta apresentada nesta dissertação buscou proporcionar aos estudantes da edu-

cação básica uma ferramenta que favoreça o aprendizado de conceitos de cibersegurança e estimule a adoção de práticas mais seguras no ambiente digital. Nesse sentido, o jogo oferece aos usuários a oportunidade de aprender a identificar e lidar com situações de risco no contexto online, além de reforçar o uso de jogos digitais como ferramentas de ensino no ambiente escolar.

Esse potencial foi evidenciado durante a intervenção, na qual os estudantes tiveram contato com conteúdos de cibersegurança por meio de um jogo digital e reconheceram sua importância como recurso educacional. Ademais, destacaram a necessidade de maior inserção desse tipo de ferramenta no contexto escolar.

Apesar das contribuições apresentadas, alguns desafios ainda persistem. A limitação de infraestrutura em muitas escolas públicas do país continua sendo um fator restritivo para a adoção de ferramentas educacionais digitais. No contexto deste estudo, por exemplo, não foi possível realizar a aplicação do jogo de forma online, o que facilitaria a coleta automática de *logs*, sendo necessária sua execução de forma totalmente *offline*.

Além disso, há desafios relacionados à adaptação de conteúdos complexos de cibersegurança para o contexto educacional básico, especialmente para estudantes em processo inicial de letramento. Esse fator pode ter impactado o desempenho em determinadas atividades da pesquisa, como aquelas relacionadas a ataques de *phishing*, nas quais parte dos estudantes, principalmente os mais novos, apresentou dificuldades de compreensão.

Por fim, persistem desafios relacionados à inclusão de estudantes com perfis neurodivergentes. Elementos como a necessidade de tomada de decisões rápidas, a alta frequência de repetição de tentativas após falhas e a ocorrência de *feedbacks* desmotivadores, somados à ausência de níveis graduais de dificuldade, podem ter influenciado negativamente a experiência desses jogadores. Esses fatores, em diversos casos, podem ter contribuído para a não conclusão das atividades por parte desses usuários.

7.1 Principais Contribuições

Esta pesquisa vai além de sua contribuição técnico-científica ao apresentar uma ferramenta tecnológica voltada para o ensino de cibersegurança, validada junto ao seu público-alvo em um contexto educacional real. Diferentemente de abordagens puramente conceituais, este trabalho busca preencher uma importante lacuna identificada na literatura: a escassez de estudos empíricos conduzidos com o público-alvo em pesquisas sobre jogos digitais educacionais voltados ao ensino básico. Em muitos casos, essas avaliações são pouco realizadas e, quando conduzidas, ocorrem com públicos mais maduros, o que pode limitar a representatividade dos resultados para estudantes da educação básica.

Nesse sentido, este estudo contempla não apenas o desenvolvimento da solução, mas também sua aplicação prática e avaliação empírica, permitindo uma análise mais consistente de seus impactos no processo de aprendizagem.

Além disso, considerando as lacunas identificadas na análise comparativa dos trabalhos correlatos, esta pesquisa contribui ao integrar diferentes aspectos frequentemente abordados de forma isolada na literatura. O jogo desenvolvido contempla os oito critérios definidos na Seção 3.3, envolvendo avaliação do aprendizado, usabilidade, experiência do jogador, utilização de *logs* de interação, disponibilidade multiplataforma, abrangência dos conteúdos de cibersegurança abordados, possibilidade de personalização e execução em modo *offline*. Dessa forma, a proposta apresenta uma abordagem mais abrangente para o desenvolvimento e avaliação de jogos digitais educacionais voltados à cibersegurança, combinando aspectos pedagógicos, técnicos e de acessibilidade em uma única solução.

Para além disso, essa pesquisa traz uma relevante contribuição social, ao se configurar como um recurso lúdico e gratuito para o letramento em cibersegurança. Os resultados demonstram que a solução pode ser utilizada como complemento ao currículo escolar, contribuindo para a alfabetização digital desde os anos iniciais do ensino básico.

Dessa forma, a proposta contribui para que os estudantes se tornem agentes multiplicadores de conhecimento, ampliando o alcance dos conceitos aprendidos para além do ambiente escolar.

7.2 Trabalhos Futuros

Como melhorias para trabalhos futuros, destaca-se a necessidade de aprimorar aspectos relacionados à interface e à experiência do usuário. Foram identificadas oportunidades de melhoria no acompanhamento do progresso em determinadas fases, bem como no *feedback* fornecido aos jogadores, recomendando-se a redução do impacto de mensagens negativas e o ajuste do nível de dificuldade para atender a diferentes perfis de jogadores.

No que tange aos elementos de jogos do *software* proposto, sugere-se a implementação de sistemas de conquistas e possibilidades de personalização, incluindo conteúdos desbloqueáveis e um sistema de progressão mais estruturado, com recompensas visuais, como *skins* e acessórios para os personagens. Além disso, recomenda-se revisar as mecânicas que demandam maior coordenação motora, a fim de tornar os desafios apresentados pela ferramenta mais equilibrados e acessíveis aos usuários.

Quanto ao aspecto pedagógico, propõe-se a refatoração da apresentação dos conteúdos técnicos nos diálogos, priorizando elementos visuais e a redução da densidade textual para estudantes mais novos, ao mesmo tempo em que se sugerem desafios com maior complexidade e autonomia para estudantes de níveis mais avançados.

No campo da inclusão, é importante expandir o jogo para atender estudantes com necessidades especiais, uma vez que a versão atual ainda não contempla plenamente recursos de acessibilidade que garantam a inclusão de todos os perfis de usuários.

Por fim, vislumbra-se a realização de um estudo longitudinal para verificar a retenção do conhecimento ao longo do tempo, além de propor estratégias para a integração

sistemática de jogos digitais de cibersegurança em disciplinas formais do currículo escolar.

7.3 Contribuições em Produção Bibliográfica

Além do desenvolvimento e da disponibilização do jogo digital educacional para uso da comunidade, este trabalho resultou nas seguintes publicações científicas:

- ❑ **Artigo completo publicado no XXIII Simpósio Brasileiro de Jogos e Entretenimento Digital (SBGames) - "Encrypta: A missão da liga dos robôs" - Um jogo educacional para aprendizagem em cibersegurança**, que apresenta o jogo digital educacional Encrypta, contribuindo para a literatura sobre jogos educacionais e conscientização em cibersegurança (ABREU; MIANI; NOMURA, 2024).
- ❑ **Artigo completo aceito para publicação no XXXII Workshop de Informática na Escola (WIE) - "Relato de uma Intervenção Pedagógica em Cibersegurança com o Jogo Digital Encrypta para Estudantes do Ensino Fundamental I e II"**, que apresenta o relato de experiência durante a aplicação do jogo no CAp/UFU.

Referências

ABREU, J. **Encrypta: A missão da liga dos robôs**. 2026. Disponivel em: <https://jeanluca-a.itch.io/encrypta-20>. Acessado em 23 de janeiro de 2026.

ABREU, J.; MIANI, R.; NOMURA, S. "Encrypta: A missão da liga dos robôs" - um jogo educacional para aprendizagem em cibersegurança. In: **Anais do XXIII Simpósio Brasileiro de Jogos e Entretenimento Digital**. Porto Alegre, RS, Brasil: SBC, 2024. p. 1327–1338. DOI: https://doi.org/10.5753/sbgames.2024.240133.

AMJAD, K. et al. Unlocking cybersecurity: A game-changing framework for training and awareness—a systematic review. **Human Behavior and Emerging Technologies**, Wiley Online Library, v. 2025, n. 1, p. 9982666, 2025. DOI: https://doi.org/10.1155/hbe2/9982666.

ANA, W. P. S.; LEMOS, G. C. Metodologia científica: a pesquisa qualitativa nas visões de lüdke e andré. **Revista Eletrônica Científica Ensino Interdisciplinar**, v. 4, n. 12, 2018. DOI: https://doi.org/10.21920/recei72018412531541.

BATTISTELLA, P. E.; WANGENHEIM, C. G. von. Engaged: Um processo de desenvolvimento de jogos para ensinar computaçao. In: **Brazilian Symposium on Computers in Education (Simpósio Brasileiro de Informática na Educação-SBIE)**. Uberlândia, MG: SBC, 2016. v. 27, n. 1, p. 380. DOI: https://doi.org/10.5753/cbie.sbie.2016.380.

BEDWELL, W. L. et al. Toward a taxonomy linking game attributes to learning: An empirical study. **Simulation & Gaming**, v. 43, n. 6, p. 729–760, 2012. Disponível em: <https://doi.org/10.1177/1046878112439444>.

BERNARDINO, I. et al. Desenvolvimento do jogo sério web segura. **Rotura–Revista de Comunicação, Cultura e Artes**, v. 3, n. 1, p. 74–101, 2023.

BRASIL - Ministério da Educação. **Parecer CNE/CEB nº 2/2022: Normas sobre Computação na Educação Básica – Complemento à Base Nacional Comum Curricular (BNCC)**. Brasília, DF, 2022. Disponível em: <https://www.gov.br/mec/pt-br/cne/pdf/pareceres-do-cne/ceb/2022/pceb002_22.pdf>. Acesso em: 27 abr. 2026.

BUSSAB, W. d. O.; MORETTIN, P. A. **Estatística básica**. 6. ed. São Paulo: Saraiva, 2010. xvi–540 p.

CABRAL, L. M.; FIGUEIREDO, C. L. F. Os avanços dos crimes cibernéticos e a lacuna existente na legislação brasileira. UCSal-Universidade Católica do Salvador, Salvador, BA, 2025.

CARDOSO, V. W. **Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo Phishing**. 2024. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal do Rio de Janeiro (UFRJ).

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br). **TIC Kids Online Brasil 2024: Principais Resultados**. São Paulo, 2024. Disponível em: <https://cetic.br/media/analises/tic_kids_online_brasil_2024_principais_resultados.pdf>.

Check Point. Technical Report, **Cyber Security Report 2026**. 2026. Disponivel em: url=https://www.checkpoint.com/security-report/. Acessado em 26 de abril de 2025.

Chosic. **Royalty-free music**. 2026. Disponivel em: <https://www.chosic.com/>. Acessado em 10 de março de 2026.

COELHO, P. M. F.; COSTA, M. R. M.; VALENTE, J. A. Currículo e jogos digitais educativos: possibilidades de articulação de demandas sociais. **Revista da FAEEBA-Educação e Contemporaneidade**, v. 32, n. 71, p. 344–361, 2023. DOI: https://doi.org/10.21879/faeeba2358-0194.2023.v32.n71.p344-361.

COHEN, J. **Statistical Power Analysis for the Behavioral Sciences**. 2nd. ed. New York: Routledge, 1988.

CORRÊA, E. C. C.; SILVA, E. S. et al. Crimes cibernéticos características, peculiaridades da investigação e as ameaças na ‘’rede mundial de computadores”. Pontifícia Universidade Católica de Goiás, Goiânia, GO, 2023.

CÔRTES, A. J. M. da R.; PAIXÃO, E. d. S. de B. Uso de jogos digitais na educação básica: Análise das abordagens sobre aplicações no contexto escolar nos anos de 2017 a 2020. **Revista Inter-Ação**, v. 48, n. 3, p. 1013–1024, 2023. DOI: https://doi.org/10.5216/ia.v48i3.75883.

CSIKSZENTMIHALYI, M. **Flow: The Psychology of Optimal Experience**. New York: Harper & Row, 1990.

DAMENU, T. K. et al. Cyber security educational games for children: A systematic literature review. **arXiv preprint arXiv:2508.17414**, 2025.

DataReportal. **Digital 2026: Brazil**. 2026. Acesso em: 29 de abril de 2026. Disponível em: <https://datareportal.com/reports/digital-2026-brazil>.

DIAS, A. et al. O uso de quizzes como ferramenta para educação em cibersegurança. In: **Anais da I Escola Regional de Sistemas de Informação de Mato Grosso**. Porto Alegre, RS, Brasil: SBC, 2025. p. 91–101. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/ersimt/article/view/35790>.

FARIAS, F. et al. Self protect: Um jogo para auxílio no ensino de conceitos relacionados a segurança na internet para crianças e adolescentes. In: **Anais do XXV Workshop de Informática na Escola**. Porto Alegre, RS, Brasil: SBC, 2019. p. 246–255. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/wie/article/view/13172>.

FELCHER, C. D. O.; FOLMER, V. EducaÇÃo 5.0: ReflexÕes e perspectivas para sua implementaÇÃo. **Revista Tecnologias Educacionais em Rede (ReTER)**, v. 2, n. 3, p. e5/01–15, out. 2021. Disponível em: <https://periodicos.ufsm.br/reter/article/view/67227>.

FERREIRA, A. L. H. et al. Características dos jogos sérios anti-phishing como ferramenta de ensino: uma revisão sistemática. **Revista Novas Tecnologias na Educação**, v. 22, n. 1, p. 340–350, 2024. DOI: https://doi.org/10.22456/1679-1916.141560.

FILHO, M. A. S. de A. et al. Educação 5.0: Além da tecnologia, o humano no centro. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 7, p. 186–194, 2025. DOI: https://doi.org/10.51891/rease.v11i7.20235.

FONSECA, A. B. B. N. da et al. Do quadro negro ao digital: Vantagens na aprendizagem contemporânea. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 4, p. 1034–1041, 2025. DOI: https://doi.org/10.51891/rease.v11i4.18738.

FREDRICKS, J. A.; BLUMENFELD, P. C.; PARIS, A. H. School engagement: Potential of the concept, state of the evidence. **Review of Educational Research**, [Sage Publications, Inc., American Educational Research Association], v. 74, n. 1, p. 59–109, 2004. ISSN 00346543, 19351046. DOI: https://doi.org/10.3102/00346543074001059. Disponível em: <http://www.jstor.org/stable/3516061>.

FRYDMAN, D. D.; BUENO, N. d. M. Desenvolvimento de um jogo mobile para ensino de segurança da informação utilizando flutter. Universidade Federal Fluminense (UFF), Niterói, RJ, 2023.

FURTADO, G. de O.; SOTIL, J. W. C. A utilização de jogos educativos digitais no processo de ensino: Vantagens e desafios. **Revista Científica FESA**, v. 3, n. 14, p. 153–163, 2024. DOI: https://doi.org/10.56069/2676-0428.2024.390.

GIL, A. C. **Pesquisa social**. 4. ed. São Paulo: Atlas, 1995.

GWENHURE, A. K.; RAHAYU, F. S. Gamification of cybersecurity awareness for non-it professionals: A systematic literature review. **International Journal of Serious Games**, v. 11, n. 1, p. 83–99, 2024. DOI: https://doi.org/10.17083/ijsg.v11i1.719.

HAIR, J. F. et al. **Análise multivariada de dados**. Porto Alegre: Bookman editora, 2009.

HAKEA, R. R. Interactive-engagement versus traditional methods: a sixthousand-student survey of mechanics test data for introductory physics courses. **Am J Phys**, v. 66, p. 64–67, 1998. DOI: https://doi.org/10.1119/1.18809.

IBGE. **Instituto Brasileiro de Geografia e Estatística - Censo 2022**. 2025. Disponivel em: <https://www.ibge.gov.br/>. Acessado em 29 de setembro de 2025.

INAGAKI, J. Y. M. **Cibercrimes relacionados às crianças e adolescentes**. Higienópolis, SP, Brasil, 2023. Trabalho de Conclusão de Curso. Universidade Presbiteriana Mackenzie.

Itch.io. **Website for indie games and creative resources**. 2026. Disponivel em: <https://itch.io/>. Acessado em 20 de janeiro de 2026.

JUNIOR, E. W. S. V. Ensino de segurança da informação no fundamental 1: uso de ia e laboratórios virtuais como ferramentas. **Monumenta-Revista Científica Multidisciplinar**, v. 10, n. 10, p. 324–341, 2024. DOI: https://doi.org/10.57077/monumenta.v10i10.274.

JÚNIOR, J. F. et al. 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**. Porto Alegre, RS, Brasil: SBC, 2024. p. 219–232. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/30140>.

KELLER, J. M. Development and use of the arcs model of motivational design. **Journal of Instructional Development**, v. 10, n. 3, p. 2–10, 1987. DOI: https://doi.org/10.1007/BF02905780.

KORKIAKOSKI, M. et al. Hack the room: Exploring the potential of an augmented reality game for teaching cyber security. In: **Proceedings of the Augmented Humans International Conference 2023**. New York, NY, USA: ACM, 2023. p. 349–353. DOI: https://doi.org/10.1145/3582700.3583955.

KOSTIC, M.; SAVELJIC, I. Interactive cybersecurity awareness: Creating a gamified password strength checker with unity. CEUR-WS.org, v. 3971, p. 43–52, 2024. Disponível em: <http://dblp.uni-trier.de/db/conf/bisec/bisec2024.html#KosticS24>.

LEVENE, H. Robust tests for equality of variances. **Contributions to probability and statistics**, Stanford University Press, p. 278–292, 1960.

MARCONI, M. d. A.; LAKATOS, E. M. **Metodologia científica**. São Paulo: Atlas, 2004. v. 4.

MCNEMAR, Q. Note on the sampling error of the difference between correlated proportions or percentages. **Psychometrika**, Springer-Verlag, v. 12, n. 2, p. 153–157, 1947. DOI: https://doi.org/10.1007/BF02295996.

MEIRELLES, F. S. **Pesquisa do uso da TI-tecnologia de informação, 36a Pesquisa Anual**. São Paulo, 2025. Fundação Getulio Vargas - FGVcia. Disponível em: <https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti_fgvcia_2025.pdf>.

MixKit. **Royalty-free music and sound effects**. 2026. Disponivel em: <https://mixkit.co/>. Acessado em 10 de março de 2026.

MONTE, J. P. P. do; NOVAIS, R. B. P. G. Princípios da educação clássica e a efetivação do direito à educação no brasil contemporâneo: Uma abordagem jurídica, filosófica e pedagógica. In: **Anais do 26º Seminário de Pesquisa do CCSA**. Natal, RN: UFRN, 2024.

NG, C. Y.; HASAN, M. K. B. Cybersecurity serious games development: A systematic review. **Computers & Security**, v. 150, p. 104307, 2025. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404824006138>.

OVIGLI, D. et al. Jogos digitais comerciais, emoções e educação: Um estado da arte de 2002 a 2022. **Igapó**, v. 19, n. 1, 2025.

PAPERT, S. **Children, computers, and powerful ideas**. Eugene, OR, USA: Harvester, 1980. v. 10.

PEFFERS, K. et al. A design science research methodology for information systems research. **Journal of management information systems**, Taylor & Francis, v. 24, n. 3, p. 45–77, 2007. DOI: https://doi.org/10.2753/MIS0742-1222240302.

PERDIZ, K. A.; NETO, C. C. G. Cibercriminalidade e infância na era digital: um estudo sobre a bahia no período entre 2023 e 2024. UCSal, Universidade Católica do Salvador, 2025.

PETRI, G.; WANGENHEIM, C. von; BORGATTO, A. Meega+: Um modelo para a avaliação de jogos educacionais para o ensino de computação. **Revista Brasileira de Informática na Educação**, v. 27, n. 03, p. 52–81, 2019. ISSN 2317-6121. Disponível em: <http://milanesa.ime.usp.br/rbie/index.php/rbie/article/view/v27n035281>.

PIAGET, J. **Piaget's theory**. New York, NY: Springer, 1976. DOI: https://doi.org/10.1007/978-3-642-46323-5_2.

PIETRUCHINSKI, M. H. et al. Os jogos educativos no contexto do sbie: uma revisão sistemática de literatura. In: **Brazilian Symposium on Computers in Education (Simpósio Brasileiro de Informática na Educação-SBIE)**. Aracaju, SE: SBC, 2011. v. 1, n. 1.

ROLLWAGEN, A. F. et al. Software educacional para levantamento de requisitos de software. **Salão do Conhecimento**, UNIJUÍ, Ijuí, v. 6, n. 6, 2020.

ROMÃO, A. A. et al. Educação 5.0: O humano no centro da inovação. **Missioneira**, v. 27, n. 9, p. 317–329, 2025. DOI: https://doi.org/10.46550/vzvb4158.

SANTOS, E. E. dos et al. Cyber defender: desenvolvimento e avaliação de um jogo educativo para ensino de segurança cibernética. In: SBC. **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. Foz do Iguaçu, PR, 2025. p. 289–304. DOI: https://doi.org/10.5753/sbseg.2025.10588.

SCHÜNEMANN, L. H. A.; GARCIA, T. R. Aplicabilidade de jogos digitais comerciais na educaçao: Uma revisao da literatura. **Anais do XXXIV Simpósio Brasileiro de Informática na Educação**, SBC, Passo Fundo, RS, p. 752–763, 2023. DOI: https://doi.org/10.5753/sbie.2023.234787.

SHAPIRO, S. S.; WILK, M. B. An analysis of variance test for normality (complete samples). **Biometrika**, Oxford University Press, v. 52, n. 3-4, p. 591–611, 1965. DOI: https://doi.org/10.1093/biomet/52.3-4.591.

SILVA, B. M. A. da et al. Estatuto da criança e do adolecente e os crimes cibernético. **Revista Mais Palmeiras**, v. 1, n. 1, p. 106–118, 2025.

SILVA, T. R. da; MEDEIROS, T. J.; ARANHA, E. H. d. S. Jogos digitais para ensino e aprendizagem de programação: uma revisão sistemática da literatura. In: **Brazilian Symposium on Computers in Education (Simpósio Brasileiro de Informática na Educação-SBIE)**. Dourados, MS: SBC, 2014. v. 25, n. 1, p. 692. DOI: https://doi.org/10.5753/cbie.sbie.2014.692.

SOUTO, M.; SILVA, C. Um catálogo de requisitos pedagógicos para auxiliar o desenvolvimento de softwares educacionais. In: **Anais do Simpósio Brasileiro de Informática na Educação (SBIE)**. Recife, PE: SBC, 2017. p. 506. DOI: https://doi.org/10.5753/cbie.sbie.2017.506.

SOUZA, L. C. de; TANAKA, S. S. Estudo sobre ataques de phishing e suas técnicas de defesa. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, v. 39, n. especial, p. 90–95, 2023.

SOUZA, M. et al. Cyber resistance: Protótipo de jogo educacional para ensino de segurança cibernética. In: **Anais Estendidos do XXV Simpósio Brasileiro de Cibersegurança**. Porto Alegre, RS, Brasil: SBC, 2025. p. 305–311. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/36769>.

SOUZA, N. R. S. de et al. Prevenção de golpes digitais: O papel da cibersegurança na proteção do usuário. In: SBC. **Conferência de Tecnologia do ICET (CONNECTech)**. Itacoatiara, AM, 2025. p. 236–248. DOI: https://doi.org/10.5753/connect.2025.12176.

SPEARMAN, C. The proof and measurement of association between two things. Appleton-Century-Crofts, 1961. DOI: https://doi.org/10.1037/11491-005.

TEIXEIRA, G. C. A. Educação digital na escola: Cultura de paz e cidadania digital. **Guarita Digital**, 2023. DOI: https://doi.org/10.29327/5276539.1-14.

Trend Micro. Technical Report, **TREND 2025 CYBER RISK REPORT**. 2025. Disponivel em: url=https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-2025-cyber-risk-report. Acessado em 26 de abril de 2025.

VASCONCELOS, L.; PRADO, V. do; BARBIERI, N. Reflexões sobre a educação digital como direito fundamental para o exercício da cidadania. **Direito UNIFACS–Debate Virtual-Qualis A2 em Direito**, n. 281, 2023.

VYGOTSKY, L. S. Imagination and creativity in the adolescent. **Soviet Psychology**, Taylor & Francis, v. 29, n. 1, p. 73–88, 1991. DOI: https://doi.org/10.2753/RPO1061-0405290173.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier, 2009. v. 2.

WILCOXON, F. Individual comparisons by ranking methods. **Biometrics bulletin**, JSTOR, v. 1, n. 6, p. 80–83, 1945. DOI: https://doi.org/10.2307/3001968.

ZANOTTI, E. d. S. S. A importância das ferramentas digitais no processo de ensino e aprendizagem pós covid-19. **OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA**, v. 23, n. 9, p. e11404–e11404, 2025. DOI: https://doi.org/10.55905/oelv23n9-052.

Apêndices

APÊNDICE **A**

Questionário Pré/Pós-Teste

Universidade Federal de Uberlândia
FACOM - FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIENCIA DA COMPUTAÇÃO

Teste de Conhecimento 1

Sexo: ( ) Masculino ( ) Feminino **Idade: _____**
Turma: ( ) 4° ano ( ) 5° ano ( ) 6° ano ( ) 7° ano

Qual das seguintes opções é considerada uma senha forte?

☐ 12345678910 ☐ s@Gwa0rE23L6 ☐ abcd1234 ☐ QeTrwy15

Qual é a recomendação mais segura para criar uma senha forte?

☐ Usar letras minúsculas e maiúsculas, números e emojis
☐ Usar letras maiúsculas, minúsculas, números e caracteres especiais
☐ Usar a mesma senha para várias contas
☐ Escolher palavras comuns do dicionário

Qual é o comprimento mínimo recomendado para uma senha forte?

☐ 8 caracteres ☐ 12 caracteres ☐ 10 caracteres

O que é phishing?

☐ Um método para proteger seu computador de vírus
☐ Uma tentativa de enganar os usuários para obter informações pessoais
☐ Uma técnica para enviar emails não solicitados

Como você pode identificar um email de phishing?

☐ Respondendo o email
☐ Abrindo todos os anexos
☐ Olhando para o remetente do e-mail e para possíveis erros de português
☐ Clicando em todos os links presentes no email

O que você deve fazer se receber um email suspeito?

☐ Responder com suas informações pessoais
☐ Excluí-lo e não clicar em nenhum link ou anexo
☐ Encaminhar para todos os seus contatos
☐ Ler o email e deixá-lo armazenado para futuras verificações

O que você deve fazer antes de abrir um anexo de email?

☐ Verificar se o remetente é confiável
☐ Abrir imediatamente
☐ Habilitar o antivírus para proteção

Qual destes pode ser um arquivo malicioso?

☐ Um documento PDF obtido no site oficial da escola

- ☐ Um jogo pirata baixado de um site desconhecido
- ☐ Uma música em formato MP3 reproduzida por um aplicativo de streaming autorizado
- ☐ Um vídeo educativo em MP4 enviado pelo professor via Google Drive

Como evitar obter arquivos maliciosos?

- ☐ Evitando fazer downloads de sites não confiáveis e clicar em links suspeitos em emails ou mensagens
- ☐ Baixando arquivos de fontes desconhecidas sem verificar sua autenticidade
- ☐ Abrindo todos os anexos de emails sem pensar duas vezes
- ☐ Nenhuma das alternativas

Qual é o protocolo mais seguro para navegar na web?

☐ HTTP ☐ SSH ☐ HTTPS ☐ FTPa

O que o HTTPS indica em um site?

- ☐ Garantir que o site seja seguro e legítimo
- ☐ Garantir que o site seja gratuito
- ☐ Garantir que o site seja malicioso

Por que fazer backup regularmente é importante?

- ☐ Para proteger contra a perda de dados devido a falhas do computador ou do celular
- ☐ Para economizar espaço de armazenamento
- ☐ Para perder dados importantes

Qual é a melhor prática para fazer backup de dados?

- ☐ Fazer backup uma vez por ano
- ☐ Fazer backup de arquivos pequenos
- ☐ Fazer backup regularmente e armazenar cópias em locais seguros
- ☐ Não fazer backup de dados, pois só é necessário em certas ocasiões

O que você deve fazer se perder seus dados devido a um problema no computador?

- ☐ Restaurar os dados de um backup recente
- ☐ Realizar backup dos dados perdidos
- ☐ Nada, os dados estão perdidos para sempre
- ☐ Continuar usando o computador sem se preocupar com os dados perdidos

Como garantir a segurança dos seus dados online?

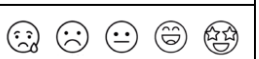
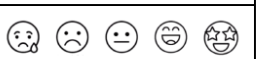
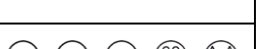
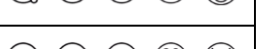
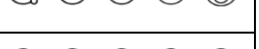
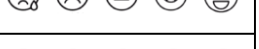
- ☐ Usar senhas fortes e únicas, fazer backup regularmente e ser cauteloso ao abrir emails e arquivos suspeitos
- ☐ Se conectar em redes de Wi-Fi públicas e nunca verificar a autenticidade de emails recebidos
- ☐ Clicar em links e anexos sem verificar sua autenticidade e armazenar todas as senhas em um único local
- ☐ Ativar o backup automático de dados e compartilhar todas as senhas em um documento na nuvem

APÊNDICE **B**

Questionário MEEGA+

Questionário de Usabilidade e Experiência do Jogador

	
1. O design do jogo é atraente (interface, gráficos, tabuleiro, cartas, etc).	
2. Os textos, cores e fontes combinam e são consistentes.	
3. Eu precisei aprender poucas coisas para poder começar a jogar o jogo.	
4. Aprender a jogar este jogo foi fácil para mim.	
5. Eu acho que a maioria das pessoas aprenderiam a jogar este jogo rapidamente.	
6. Eu considero que o jogo é fácil de jogar.	
7. As regras do jogo são claras e compreensíveis.	
8. Fontes (tamanho e estilo) utilizadas no jogo são legíveis.	
9. As cores utilizadas no jogo são compreensíveis.	
10. O jogo permite personalizar a aparência (fonte e/ou cor) conforme a minha necessidade.	
11. O jogo me protege de cometer erros.	
12. Quando eu cometo um erro é fácil de me recuperar rapidamente.	
13. Quando olhei pela primeira vez o jogo, eu tive a impressão de que seria fácil para mim.	
14. A organização do conteúdo me ajudou a estar confiante de que eu iria aprender com este jogo.	
15. Este jogo é adequadamente desafiador para mim.	
16. O jogo oferece novos desafios (oferece novos obstáculos, situações ou variações) com um ritmo adequado.	

17. O jogo não se torna monótono nas suas tarefas (repetitivo ou com tarefas chatas).	
18. Completar as tarefas do jogo me deu um sentimento de realização.	
19. É devido ao meu esforço pessoal que eu consigo avançar no jogo.	
20. Me sinto satisfeito com as coisas que aprendi no jogo.	
21. Eu recomendaria este jogo para meus colegas.	
22. Eu pude interagir com outras pessoas durante o jogo.	
23. O jogo promove momentos de cooperação e/ou competição entre os jogadores.	
24. Eu me senti bem interagindo com outras pessoas durante o jogo.	
25. Eu me diverti com o jogo.	
26. Aconteceu alguma situação durante o jogo (elementos do jogo, competição, etc.) que me fez sorrir.	
27. Houve algo interessante no início do jogo que capturou minha atenção.	
28. Eu estava tão envolvido no jogo que eu perdi a noção do tempo.	
29. Eu esqueci sobre o ambiente ao meu redor enquanto jogava este jogo.	
30. O conteúdo do jogo é relevante para os meus interesses.	
31. É claro para mim como o conteúdo do jogo está relacionado com a disciplina.	
32. O jogo é um método de ensino adequado para esta disciplina.	
33. Eu prefiro aprender com este jogo do que de outra forma (outro método de ensino).	
34. O jogo contribuiu para a minha aprendizagem na disciplina.	
35. O jogo foi eficiente para minha aprendizagem, em comparação com outras atividades da disciplina.	

APÊNDICE C

TERMO DE ASSENTIMENTO PARA INDIVÍDUO ENTRE 9 E 13 ANOS INCOMPLETOS

TERMO DE ASSENTIMENTO PARA INDIVÍDUO ENTRE 9 E 13 ANOS INCOMPLETOS

Você está sendo convidado(a) a participar da pesquisa intitulada "Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional de Conscientização em Cibersegurança para Estudantes do Ensino Básico", sob a responsabilidade dos(as) pesquisadores(as) Jeanluca Martins de Abreu, Diego Nunes Molino e Rafael Dias Araujo.

Nesta pesquisa nós estamos buscando desenvolver e avaliar um jogo educacional com o objetivo de conscientizar crianças e adolescentes sobre como elas podem se proteger na internet, evitando perigos como golpes online, problemas com senhas fracas e a identificar emails e informações falsas.

O Termo/Registro de Assentimento está sendo obtido com o apoio da equipe pedagógica da ESEBA (Escola de Educação Básica da Universidade Federal de Uberlândia), que será responsável por intermediar o envio e a devolução dos termos assinados pelos estudantes. Esse processo ocorrerá antes do início da aplicação dos testes, garantindo que apenas os(as) estudantes que apresentarem o termo assinado participem da pesquisa.

Você tem o tempo que for necessário para decidir se quer ou não participar da pesquisa (conforme item IV da Resolução nº 466/2012 ou Capítulo. III da Resolução nº 510/2016).

Na sua participação, você participará de duas sessões presenciais em sala de aula: na primeira, responderá a um breve questionário sobre conceitos básicos de segurança online, na segunda jogará o jogo educacional "Encrypta" e logo em seguida responderá novamente o questionário aplicado anteriormente para avaliar o que aprendeu durante o uso do jogo, por fim responderá também a um questionário sobre a usabilidade e experiência do usuário sobre a aplicação. O tempo estimado para a primeira sessão é de cerca de 15 minutos, já o tempo estimado para a segunda sessão é de cerca de 50 minutos.

Você tem o direito de não responder qualquer questão, sem necessidade de explicação ou justificativa para tal.

Você não terá nenhum gasto nem ganho financeiro por participar na pesquisa.

Nós, pesquisadores, atenderemos as orientações das Resoluções nº 466/2012, Capítulo XI, Item XI.2: f e nº 510/2016, Capítulo VI, Art. 28: IV - manter os dados da pesquisa em arquivo, físico ou digital, sob sua guarda e responsabilidade, por um período mínimo de 5 (cinco) anos após o término da pesquisa.

Os resultados da pesquisa serão publicados, e ainda assim a sua identidade será preservada. Os dados coletados serão armazenados digitalmente com senha e acesso restrito aos(as) pesquisadores(as), por no mínimo 5 anos. Não serão divulgadas informações pessoais, e o participante não precisará informar seu nome durante todo o processo de participação da pesquisa.

Os riscos consistem em: os riscos são mínimos, limitando-se ao possível desconforto em responder perguntas ou jogar na frente dos colegas. Para minimizar isso, a participação será voluntária, e o(a) estudante poderá parar a qualquer momento. Não serão coletadas informações sensíveis.

Os benefícios serão: o(a) participante poderá aprender a se proteger melhor na internet e desenvolver hábitos mais seguros ao usar computadores e celulares. A sociedade também será beneficiada com a criação de uma ferramenta gratuita de educação digital.

Você é livre para deixar de participar da pesquisa a qualquer momento sem qualquer prejuízo ou coação, bem como não é obrigado a participar da mesma se não quiser. Entretanto, como os questionários serão respondidos de forma anônima, **não será possível identificar e, portanto, excluir os dados fornecidos após o envio das respostas**.

Uma via original deste Termo de Assentimento ficará com você, assinada e rubricada pelos(as) pesquisadores(as).

Em qualquer momento, caso tenha qualquer dúvida ou reclamação a respeito da pesquisa, você poderá entrar em contato com o pesquisador responsável:

Jeanluca Martins de Abreu

Universidade Federal de Uberlândia – Instituto de Informática

E-mail: jeanluca.abreu@ufu.br | Telefone: (31) 99557-4087

Havendo algum dano decorrente da pesquisa, você tem direito a solicitar indenização através das vias judiciais (Código Civil, Lei 10.406/2002, Artigos 927 a 954 e Resolução CNS nº 510 de 2016, Artigo 19).

Para obter orientações quanto aos direitos dos participantes de pesquisa acesse a cartilha disponível no *link*: https://propp.ufu.br/sites/propp.ufu.br/files/media/documento/cartilha_dos_direitos_dos_participantes_de_pesquisa.pdf

Você poderá também entrar em contato com o Comitê de Ética na Pesquisa com Seres Humanos – CEP, da Universidade Federal de Uberlândia, localizado na Av. João Naves de Ávila, nº 2121, bloco A, sala 224, *campus* Santa Mônica – Uberlândia/MG, 38408-100; pelo telefone (34) 3239-4131; ou pelo *e-mail* **cep@propp.ufu.br**. O CEP/UFU é um colegiado independente criado para defender os interesses dos participantes das pesquisas em sua integridade e dignidade e para contribuir para o desenvolvimento da pesquisa dentro de padrões éticos conforme resoluções do Conselho Nacional de Saúde.

Uberlândia, ... de ..... de 20.....

_____

Assinatura do(a) pesquisador(a)

Eu aceito participar do projeto citado acima, voluntariamente, após ter sido devidamente esclarecido.

_____

Assinatura do(a) participante de pesquisa

APÊNDICE **D**

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado(a) a participar da pesquisa intitulada "Encrypta: Desenvolvimento e Avaliação de um Jogo Educacional de Conscientização em Cibersegurança para Estudantes do Ensino Básico", sob a responsabilidade dos(as) pesquisadores(as) Jeanluca Martins de Abreu, Diego Nunes Molino e Rafael Dias Araujo.

Nesta pesquisa nós estamos buscando desenvolver e avaliar um jogo educacional com o objetivo de conscientizar crianças e adolescentes sobre como elas podem se proteger na internet, evitando perigos como golpes online, problemas com senhas fracas e a identificar emails e informações falsas.

O Termo/Registro de Consentimento Livre e Esclarecido está sendo obtido com o apoio da equipe pedagógica da ESEBA (Escola de Educação Básica da Universidade Federal de Uberlândia), que será responsável por intermediar o envio e a devolução dos termos assinados pelos responsáveis legais dos estudantes. Esse processo ocorrerá antes do início da aplicação dos testes, garantindo que apenas os(as) estudantes autorizados(as) participem da pesquisa.

Você tem o tempo que for necessário para decidir se quer ou não participar da pesquisa (conforme item IV da Resolução nº 466/2012 ou Capítulo. III da Resolução nº 510/2016).

O estudante participará de duas sessões presenciais em sala de aula. Na primeira, será convidado a preencher um breve questionário sobre conceitos básicos de segurança online. Na segunda, jogará o jogo educacional "Encrypta" e, logo após, responderá novamente o questionário inicial para avaliar o conhecimento adquirido durante o uso do jogo. Por fim, também preencherá um questionário voltado à usabilidade e à experiência do usuário com a aplicação. O tempo estimado para a primeira etapa é de cerca de 15 minutos, enquanto a segunda deve durar aproximadamente 50 minutos.

O estudante tem o direito de não responder a qualquer questão, sem necessidade de explicação ou justificativa para tal.

O estudante não terá nenhum gasto nem ganho financeiro por participar da pesquisa.

Nós, pesquisadores, atenderemos às orientações das Resoluções nº 466/2012, Capítulo XI, Item XI.2: f e nº 510/2016, Capítulo VI, Art. 28: IV - manter os dados da pesquisa em arquivo, físico ou digital, sob nossa guarda e responsabilidade, por um período mínimo de 5 (cinco) anos após o término da pesquisa.

Os resultados da pesquisa serão publicados, e ainda assim a identidade do estudante será preservada. Os dados coletados serão armazenados digitalmente com senha e acesso restrito aos(as) pesquisadores(as), por no mínimo 5 anos. Não serão divulgadas informações pessoais, e o participante não precisará informar seu nome durante todo o processo de participação da pesquisa.

Os riscos consistem em: os riscos são mínimos, limitando-se ao possível desconforto em responder perguntas ou jogar na frente dos colegas. Para minimizar isso, a participação será voluntária, e o(a) estudante poderá parar a qualquer momento. Não serão coletadas informações sensíveis.

Os benefícios serão: o(a) participante poderá aprender a se proteger melhor na internet e desenvolver hábitos mais seguros ao usar computadores e celulares. A sociedade também será beneficiada com a criação de uma ferramenta gratuita de educação digital.

O estudante é livre para deixar de participar da pesquisa a qualquer momento sem qualquer prejuízo ou coação. A participação nesta pesquisa é voluntária, podendo o(a)

participante desistir a qualquer momento, sem necessidade de justificativa e sem qualquer prejuízo. Como os questionários serão respondidos de forma anônima, **não será possível identificar e, portanto, excluir os dados fornecidos após o envio das respostas**.

Uma via original deste Termo de Consentimento Livre e Esclarecido ficará com você, assinada e rubricada pelos(as) pesquisadores(as).

Em qualquer momento, caso tenha qualquer dúvida ou reclamação a respeito da pesquisa, você poderá entrar em contato com o pesquisador responsável:

Jeanluca Martins de Abreu

Universidade Federal de Uberlândia – Instituto de Informática

E-mail: jeanluca.abreu@ufu.br | Telefone: (31) 99557-4087

Havendo algum dano decorrente da pesquisa, você tem direito a solicitar indenização através das vias judiciais (Código Civil, Lei 10.406/2002, Artigos 927 a 954 e Resolução CNS nº 510 de 2016, Artigo 19).

Para obter orientações quanto aos direitos dos(as) participantes de pesquisa, acesse a cartilha disponível no *link*: https://propp.ufu.br/sites/propp.ufu.br/files/media/documento/cartilha_dos_direitos_dos_participantes_de_pesquisa.pdf

Você poderá também entrar em contato com o Comitê de Ética na Pesquisa com Seres Humanos – CEP, da Universidade Federal de Uberlândia, localizado na Av. João Naves de Ávila, nº 2121, bloco A, sala 224, *campus* Santa Mônica – Uberlândia/MG, 38408-100; pelo telefone (34) 3239-4131; ou pelo *e-mail* **cep@propp.ufu.br**. O CEP/UFU é um colegiado independente criado para defender os interesses dos(as) participantes das pesquisas em sua integridade e dignidade e para contribuir para o desenvolvimento da pesquisa dentro de padrões éticos conforme resoluções do Conselho Nacional de Saúde.

Uberlândia, ... de ..... de 20.....

_____

Assinatura do(a) pesquisador(a)

Eu aceito participar do projeto citado acima, voluntariamente, após ter sido devidamente esclarecido.

_____

Assinatura do(a) participante de pesquisa

_____ _____

Rubrica do(a) Participante Rubrica do(a) Pesquisador(a)