Revista Brasileira de Informática na Educação – RBIE
Brazilian Journal of Computers in Education
(ISSN online: 2317-6121; print: 1414-5685)
https://sol.sbc.org.br/journals/index.php/rbie

Submission: 30/Mar/2026; 1st round notif.: 24/Jun/2026; New version: 10/Jul/2026; 2nd round notif.: 23/Jul/2026;
Camera ready: 26/Jul/2026; Edition review: 04/Aug/2026; Available online: 27/Aug/2026; Published: 27/Aug/2026;

CyberQuest: avaliação de um jogo de tabuleiro como produto educacional para o ensino de segurança da informação no ensino médio

Title: CyberQuest: Evaluation of a Board Game as an Educational Product for Teaching Information Security in High School

Título: CyberQuest: Evaluación de un Juego de Mesa como Producto Educativo para la Enseñanza de la Seguridad de la Información en la Escuela Secundaria

Ademar Perfoll Junior
Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí (Unidavi)
ORCID: 0009-0001-2442-4321
junior.bsn@unidavi.edu.br

André Luís Alice Raabe
Universidade do Vale do Itajaí (Univali)
ORCID: 0000-0002-8093-2507
raabe@univali.br

Resumo
Este artigo investiga a aplicação do jogo de tabuleiro CyberQuest como produto educacional para o ensino de segurança da informação no ensino médio. Com base na abordagem Design-Based Research (DBR), analisa evidências produzidas em contexto escolar real a partir do uso do jogo com 68 estudantes de duas escolas. Elaborado em alinhamento à BNCC e às normas de Computação na Educação Básica (2022), o CyberQuest promove aprendizagem situada por meio de decisões e discussão colaborativa sobre temas como phishing, malware, autenticação e privacidade. A produção de dados combinou observação participante, questionário de perfil e grupo focal. Os resultados evidenciam alto engajamento e indícios de aprendizagem situada, além de aspectos de design que influenciam a experiência didática. O trabalho demonstra que jogos de tabuleiro podem ser recursos consistentes para promover cidadania digital no ensino médio, articulando ludicidade, mediação pedagógica e reflexão crítica.
Palavras-chave: *Jogos de Tabuleiro; Segurança da Informação; Design-Based Research; Ensino Médio*

Abstract
This paper investigates the application of the CyberQuest board game as an educational product for teaching information security in high school. Drawing on the Design-Based Research (DBR) approach, it analyzes evidence produced in authentic school settings through the use of the game with 68 students from two schools. Designed in alignment with the Brazilian BNCC and the 2022 Computing in Basic Education guidelines, CyberQuest fosters situated learning through decision-making and collaborative discussion of topics such as phishing, malware, authentication, and privacy. Data production combined participant observation, a profile questionnaire, and focus groups. Results indicate high engagement and signs of situated learning, as well as design aspects that affect the didactic experience. The study demonstrates that board games can be consistent resources for fostering digital citizenship in high school by articulating playfulness, pedagogical mediation, and critical reflection.
Keywords: *Board Games; Information Security; Design-Based Research; High School*

Resumen
Este artículo investiga la aplicación del juego de mesa CyberQuest como producto educativo para la enseñanza de la seguridad de la información en la escuela secundaria. Con base en el enfoque Design-Based Research (DBR),

Cite as: Perfoll Junior, A. & Raabe, A. L. A. (2026). CyberQuest: avaliação de um jogo de tabuleiro como produto educacional para o ensino de segurança da informação no ensino médio. Revista Brasileira de Informática na Educação, 34, 1489-1513. https://doi.org/10.5753/rbie.2026.7958.

analiza evidencias producidas en un contexto escolar real a partir del uso del juego con 68 estudiantes de dos escuelas. Elaborado en alineación con la BNCC y con las normas de Computación en la Educación Básica (2022), CyberQuest promueve el aprendizaje situado por medio de decisiones y de la discusión colaborativa sobre temas como phishing, malware, autenticación y privacidad. La producción de datos combinó observación participante, cuestionario de perfil y grupo focal. Los resultados evidencian un alto nivel de compromiso e indicios de aprendizaje situado, además de aspectos de diseño que influyen en la experiencia didáctica. El trabajo demuestra que los juegos de mesa pueden ser recursos consistentes para promover la ciudadanía digital en la escuela secundaria, articulando el carácter lúdico, la mediación pedagógica y la reflexión crítica.
Palabras clave: *Juegos de Mesa; Seguridad de la Información; Design-Based Research; Escuela Secundaria*

1 Introdução

A segurança da informação pode ser compreendida como o conjunto de práticas, atitudes e medidas voltadas à preservação da confidencialidade, integridade e disponibilidade das informações e dos dados pessoais em ambientes digitais[1]. A intensificação do uso de tecnologias digitais por adolescentes tem ampliado a exposição desse público a diferentes riscos associados à segurança da informação, tais como golpes virtuais, vazamento de dados, acessos indevidos, manipulação por engenharia social e violações de privacidade. Em um cenário em que interações escolares, sociais e pessoais passam crescentemente por plataformas digitais, a formação de estudantes capazes de reconhecer ameaças, avaliar consequências e adotar práticas seguras torna-se uma demanda educacional relevante. Nesse contexto, a segurança da informação deixa de ser um tema restrito ao domínio técnico e passa a integrar o campo da cidadania digital, envolvendo julgamento crítico, responsabilidade e tomada de decisão diante de situações cotidianas mediadas por tecnologia.

No Brasil, essa necessidade dialoga com a Base Nacional Comum Curricular (BNCC) e, de modo mais específico, com as Normas sobre Computação na Educação Básica que a complementam (Brasil, 2018, 2022), as quais reconhecem a cultura digital como dimensão estruturante da formação escolar e enfatizam a atuação crítica, ética e responsável no uso de tecnologias. Embora a BNCC ofereça respaldo para a abordagem do tema, sua concretização em sala de aula ainda encontra desafios didáticos importantes. Em muitos contextos, conteúdos relacionados à segurança digital aparecem de forma pontual, normativa ou descontextualizada, dificultando a construção de aprendizagens significativas. Conceitos como *phishing*[2], autenticação, privacidade, *malware*[3] e proteção de dados não se consolidam apenas pela transmissão de informações, mas exigem experiências em que os estudantes possam analisar cenários, comparar alternativas, justificar decisões e refletir sobre suas implicações.

É nesse ponto que os jogos educacionais se mostram particularmente promissores. Ao combinar regras, objetivos, feedback e participação, os jogos criam condições para uma aprendizagem mais ativa e situada. No caso dos jogos de tabuleiro, somam-se ainda características pedagógicas relevantes para o contexto escolar: interação presencial, negociação entre pares, argumentação, cooperação situacional e baixa dependência de infraestrutura digital. Em temas como segurança da informação, essas características favorecem a problematização de riscos e comportamentos em situações simuladas, permitindo que o estudante mobilize conhecimentos em um contexto próximo de sua realidade. Revisões publicadas na própria comunidade brasileira de Informática na Educação evidenciam o interesse crescente e o potencial dos jogos como recursos de ensino e aprendizagem (Silva et al., 2015).

O uso de jogos de tabuleiro insere-se no campo das metodologias ativas de ensino-aprendizagem, nas quais o estudante assume papel central na construção do conhecimento. Mais especificamente, o *CyberQuest* caracteriza-se como uma atividade desplugada (*unplugged*), ou seja, uma estratégia de gamificação que aborda conceitos de computação e segurança digital sem o uso direto de

[1] Neste trabalho, adota-se a noção de segurança da informação em sentido amplo, articulada à formação para a cidadania digital, e não restrita à dimensão técnica ou organizacional. O foco recai sobre o reconhecimento de ameaças, a proteção de dados pessoais e a tomada de decisão responsável no uso cotidiano de tecnologias.

[2] *Phishing*: técnica de fraude que utiliza mensagens fraudulentas para induzir a vítima a revelar dados sensíveis ou a clicar em links maliciosos.

[3] *Malware*: software malicioso projetado para danificar, invadir ou obter acesso não autorizado a sistemas e dados.

computadores, recorrendo a materiais físicos e à interação presencial. Essa abordagem é especialmente pertinente em contextos escolares com infraestrutura tecnológica limitada e amplia o acesso a temas de cultura digital. Revisões recentes evidenciam o crescente interesse pelo uso pedagógico de jogos de tabuleiro na educação (Gomes & Ulbricht, 2024), ainda que sua aplicação ao ensino de segurança da informação na educação básica permaneça pouco explorada.

Nesse cenário, este artigo investiga os resultados da aplicação do jogo de tabuleiro *CyberQuest* como produto educacional voltado ao ensino de segurança da informação no ensino médio. O estudo analisa evidências produzidas a partir da utilização do jogo com estudantes de duas escolas (omitido para revisão), buscando compreender como os participantes se engajam com a dinâmica proposta, que indícios de aprendizagem emergem ao longo da experiência e quais elementos do design do jogo se mostram mais relevantes para sua utilização pedagógica. Ao focalizar a aplicação do artefato em contexto real, o trabalho contribui para a discussão sobre jogos de tabuleiro na Informática na Educação e para o desenvolvimento de práticas educacionais voltadas à promoção da cidadania digital.

Apesar do crescimento de jogos educacionais para segurança da informação, ainda são escassos estudos que investigam o uso de jogos de tabuleiro voltados à cidadania digital no ensino médio em contextos escolares reais.

2 Fundamentação Teórica

Esta seção apresenta os principais referenciais que sustentam a proposta do *CyberQuest*, organizados em torno de três eixos: a aprendizagem situada, a cidadania digital e a abordagem *Design-Based Research* (DBR).

2.1 Aprendizagem situada

A noção de aprendizagem situada parte do princípio de que o conhecimento não é construído de forma isolada na mente do indivíduo, mas emerge da participação em práticas sociais contextualizadas (Lave & Wenger, 1991). Nessa perspectiva, aprender envolve engajar-se em atividades significativas, nas quais conceitos são mobilizados para interpretar situações, tomar decisões e justificar condutas. O ambiente, os pares e a própria atividade constituem elementos centrais do processo de aprendizagem, e não meros suportes externos.

Essa concepção é particularmente adequada ao ensino de segurança da informação, uma vez que comportamentos seguros não decorrem apenas da memorização de definições, mas da capacidade de reconhecer riscos e agir de forma responsável em contextos concretos. Ao simular situações próximas do cotidiano digital dos estudantes, jogos de tabuleiro como o *CyberQuest* criam condições para que conceitos de segurança sejam mobilizados em práticas situadas de decisão e argumentação, aproximando-se do modo como esses conhecimentos são efetivamente requeridos fora da escola.

2.2 Cidadania digital

O conceito de cidadania digital amplia a discussão sobre segurança da informação ao integrá-la a uma formação ética, crítica e responsável para a atuação em ambientes digitais. Mais do que dominar aspectos técnicos, espera-se que o estudante seja capaz de avaliar consequências de suas ações, respeitar direitos próprios e de terceiros e adotar postura crítica diante de riscos e dilemas do uso de tecnologias. No contexto brasileiro, essa formação encontra respaldo na BNCC e nas normas de Computação na Educação Básica, que situam a cultura digital como dimensão estruturante da formação escolar (Brasil, 2018, 2022). O *CyberQuest* alinha-se a essa perspectiva ao propor a discussão de situações que articulam segurança, responsabilidade e convivência no ambiente digital.

2.3 Segurança da informação e educação

A segurança da informação, tradicionalmente definida pela preservação da confidencialidade, integridade e disponibilidade da informação, tem ampliado seu escopo à medida que as tecnologias digitais se tornam onipresentes no cotidiano. No contexto educacional, seu ensino não se restringe a aspectos técnicos, mas envolve a formação de comportamentos seguros e a compreensão de riscos como *phishing*, engenharia social, uso indevido de dados pessoais e exposição da privacidade. Para adolescentes, que constituem um público altamente conectado e, ao mesmo tempo, vulnerável a fraudes e manipulações, essa formação assume caráter formativo e preventivo.

Abordar segurança da informação na educação básica implica traduzir conceitos frequentemente tratados de forma técnica em situações significativas e contextualizadas. Nesse sentido, estratégias que favoreçam a problematização, a tomada de decisão e a reflexão sobre práticas cotidianas mostram-se mais promissoras do que a mera transmissão de definições. É nessa direção que os jogos educacionais, ao simular dilemas e cenários de risco, oferecem um espaço seguro para que os estudantes experimentem escolhas, reconheçam ameaças e desenvolvam atitudes responsáveis diante do ambiente digital.

2.4 Design-Based Research como abordagem de investigação

A abordagem *Design-Based Research* (DBR) caracteriza-se como uma metodologia sistemática, porém flexível, voltada à melhoria de práticas educacionais por meio de ciclos iterativos de análise, design, desenvolvimento e implementação, conduzidos em colaboração com os participantes em contextos reais e orientados à produção de princípios de design contextualizados (Wang & Hannafin, 2005). Diferentemente das metodologias experimentais tradicionais, que buscam isolar variáveis em ambientes controlados, a DBR investiga os processos de aprendizagem tal como ocorrem em cenários educacionais autênticos, assumindo o contexto social, cultural e ambiental como componente central do estudo, e não como variável a ser neutralizada (Barab & Squire, 2004).

Essa opção metodológica implica um deslocamento no modo de compreender o rigor científico. Em vez de buscar exclusivamente a validade interna de estilo laboratorial, a DBR valoriza a validade ecológica, isto é, a pertinência dos resultados no ambiente real em que a aprendizagem acontece (Barab & Squire, 2004). Sua contribuição não se limita a demonstrar que uma intervenção específica funciona, mas volta-se à compreensão de *por que* e *sob quais condições* um

design é eficaz, gerando princípios de design fundamentados teoricamente e transferíveis a outros contextos (Scott et al., 2020). O rigor, nesse paradigma, é construído ao longo do tempo, por meio da triangulação de múltiplas fontes de dados e da repetição de ciclos de análise, design, avaliação e reflexão, que permitem distinguir o ruído contextual dos mecanismos efetivamente responsáveis pelos resultados (Kennedy-Clark, 2013).

Dada sua centralidade para a presente pesquisa, cabe detalhar o conceito de validade ecológica. Trata-se de uma dimensão da validade externa que expressa o grau em que os resultados de um estudo se aplicam a situações reais, e não apenas às condições artificiais de um laboratório (Barab & Squire, 2004). Sua análise costuma considerar dois componentes complementares: o realismo do ambiente, isto é, o quanto o contexto de investigação se aproxima das condições concretas em que a prática ocorre e o realismo da experiência, relativo ao quanto a atividade engaja os participantes em processos psicológicos genuínos de decisão e aprendizagem. Avaliar o *CyberQuest* em salas de aula, com suas dinâmicas sociais, restrições de tempo e heterogeneidade de turmas, favorece ambos os componentes: o jogo é examinado nas mesmas condições em que seria efetivamente utilizado, e a experiência lúdica mobiliza decisões e discussões autênticas entre os estudantes. Assume-se, assim, uma tensão inerente entre validade interna e validade ecológica, dificilmente maximizadas ao mesmo tempo (Palmér & Van Bommel, 2021): ao mover a investigação para o contexto escolar real, a DBR abre mão de parte do controle laboratorial em favor da pertinência dos resultados para a prática.

Por articular a elaboração de artefatos educacionais, sua aplicação em ambientes autênticos e a análise sistemática dos resultados, a DBR mostra-se adequada à investigação de produtos educacionais como o *CyberQuest*, cujo desenvolvimento e refinamento ocorrem em diálogo direto com o contexto escolar. A organização dos ciclos iterativos adotada neste estudo é detalhada na Seção de Método.

3 Trabalhos Relacionados

No domínio da segurança da informação, jogos educacionais têm sido utilizados com o objetivo de promover conscientização, percepção de risco e desenvolvimento de comportamentos seguros. Diferentemente de propostas centradas em treinamento técnico especializado, grande parte desses jogos busca apoiar a compreensão de situações de risco e a tomada de decisão em cenários acessíveis a públicos não especialistas. Essa orientação é particularmente pertinente ao contexto escolar, no qual a formação em segurança digital deve priorizar o reconhecimento de ameaças e a construção de atitudes responsáveis diante do uso cotidiano de tecnologias.

Entre os trabalhos relacionados, destaca-se o *Crypto Go*, proposto por González-Tablas et al. (2020), voltado ao ensino de conceitos básicos de criptografia por meio de um jogo analógico baseado em cartas e combinações. A experiência relatada pelos autores evidencia que a manipulação física dos componentes, associada à resolução de desafios, favorece a discussão conceitual entre os participantes. A Figura 1 ilustra uma sessão do jogo em contexto educacional.



Figura 1: Jogadores interagindo com o jogo *Crypto Go*.

Fonte: adaptado de González-Tablas et al. (2020).

Outro trabalho relevante é o jogo *Threats & Trade-offs*, apresentado por Stsiampkouskaya et al. (2025), que propõe uma simulação física de decisões estratégicas em uma *startup* digital sujeita a restrições financeiras e ameaças cibernéticas. A Figura 2 apresenta o tabuleiro e seus principais componentes. Nesse caso, o foco recai sobre a necessidade de equilibrar crescimento organizacional, recursos limitados e proteção da informação, tornando visíveis os *trade-offs*[4] inerentes à gestão da segurança.

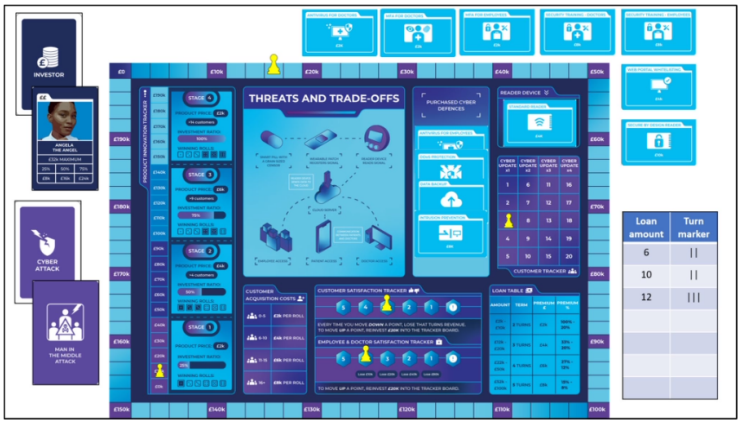


Figura 2: Jogo *Threats & Trade-offs* e seus elementos.

Fonte: adaptado de Stsiampkouskaya et al. (2025).

Os estudos mencionados indicam que jogos analógicos constituem recursos viáveis para tratar temas de segurança da informação, especialmente quando articulam tomada de decisão, interação social e contextualização dos conteúdos. Contudo, a maior parte das propostas identificadas concentra-se em conceitos específicos ou em cenários organizacionais, havendo menor presença de investigações voltadas à educação básica e ao ensino médio, com ênfase em cidadania digital e práticas de segurança associadas ao cotidiano dos jovens.

No contexto brasileiro, registram-se iniciativas governamentais e de organizações da sociedade civil que recorrem a jogos e materiais lúdicos para promover cidadania e segurança digital, como a *Trilha Cidadão Digital* (Instituto Cidadão Digital, 2025), o jogo *SerDigi*, do Serpro (Serpro, 2023), e o *Game da Cidadania*, resultado de parceria entre a Controladoria-Geral da União

[4] *Trade-off*: relação de compromisso em que a escolha de uma alternativa implica a renúncia a benefícios de outra; na gestão da segurança da informação, expressa o equilíbrio entre proteção, custo, usabilidade e recursos disponíveis.

(CGU) e a Universidade Federal de Goiás (UFG) (Controladoria-Geral da União (CGU) e Universidade Federal de Goiás (UFG), 2023). Essas propostas têm mérito reconhecido na difusão de boas práticas, mas, em geral, possuem caráter de campanha de conscientização, foco mais amplo em cidadania digital ou ética pública e pouca documentação de avaliação empírica de seu uso em sala de aula. O diferencial do *CyberQuest* está em três aspectos: (i) o foco específico em segurança da informação articulada à BNCC e ao ensino médio; (ii) a estruturação como produto educacional avaliado de forma sistemática, em contexto escolar real, sob a abordagem DBR; e (iii) a centralidade da mediação pedagógica como elemento que transforma a experiência lúdica em oportunidade de reflexão crítica. Assim, mais do que oferecer um novo jogo, o trabalho contribui com evidências sobre como esse tipo de artefato opera pedagogicamente em sala de aula.

É nesse contexto que se situa o *CyberQuest*. O jogo foi desenvolvido para abordar, em ambiente escolar, situações próximas da realidade dos estudantes, como links suspeitos, aplicativos, exposição de dados, autenticação, *malware* e privacidade, organizadas em uma dinâmica lúdica presencial mediada pedagogicamente. Assim, em vez de focar apenas na apresentação de conceitos, o jogo busca mobilizar discussão, argumentação e reflexão crítica em torno de situações contextualizadas. A investigação de seus resultados contribui, portanto, para ampliar a compreensão sobre o papel de jogos de tabuleiro como tecnologias educacionais na formação para a segurança da informação no ensino médio.

4 O Jogo CyberQuest como Produto Educacional

O *CyberQuest* é um jogo de tabuleiro elaborado para apoiar o ensino de segurança da informação no ensino médio por meio de uma experiência lúdica estruturada em torno da narrativa "Conta Segura". No jogo, cada participante assume o papel de um "Defensor da Conta Segura" e percorre um tabuleiro composto por desafios, ameaças, eventos coletivos e momentos de recuperação, simulando situações comuns do cotidiano digital contemporâneo.

A proposta pedagógica do jogo está ancorada na ideia de que conteúdos relacionados à segurança digital podem ser mais bem compreendidos quando mobilizados em situações de decisão, confronto de argumentos e avaliação de consequências. Nesse sentido, o *CyberQuest* organiza a experiência de aprendizagem em torno de interações sociais e problemas contextualizados, articulando ludicidade, regras e mediação docente.

4.1 Objetivos educacionais e exemplos de cartas

O jogo foi estruturado para mobilizar quatro objetivos educacionais principais: (i) identificar ameaças digitais comuns; (ii) compreender conceitos fundamentais de segurança da informação; (iii) estimular atitudes de prevenção, cooperação e responsabilidade digital; e (iv) desenvolver habilidades de tomada de decisão diante de situações típicas do cotidiano digital juvenil.

O primeiro objetivo (**OE1**) refere-se ao reconhecimento de ameaças digitais recorrentes. A Figura 3 apresenta exemplos das cartas do jogo com o objetivo de identificar ameaças digitais, destacadas como *(1) phishing*, (2) engenharia social e (3) softwares maliciosos.

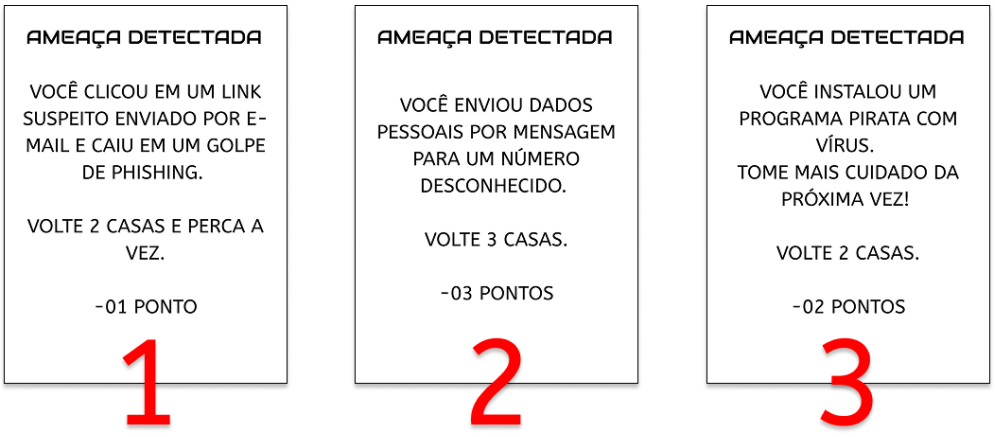


Figura 3: Exemplos de cartas voltadas à identificação de ameaças digitais comuns.

O segundo objetivo (**OE2**) diz respeito à compreensão de conceitos fundamentais, como autenticação, criptografia e proteção de dados, apresentados em cartas que demandam interpretação e associação conceitual, conforme ilustrado na Figura 4, que apresenta exemplos de conceitos de segurança da informação, como (1) autenticação, (2) criptografia e (3) proteção de dados.

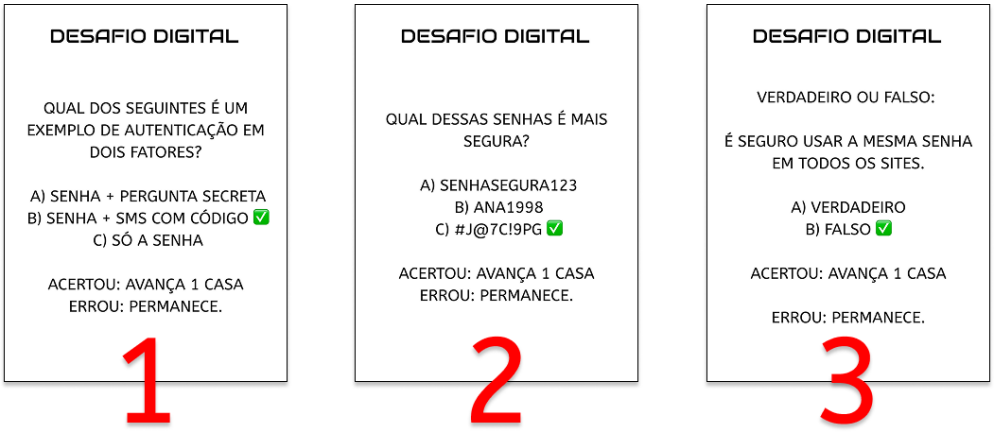


Figura 4: Exemplos de cartas voltadas à compreensão de conceitos fundamentais de segurança da informação.

O terceiro objetivo (**OE3**) está relacionado à promoção de atitudes de prevenção, cooperação e responsabilidade digital. As cartas desse eixo abordam, por exemplo, *backup*, prevenção de incidentes e consequências de vazamentos de dados, como mostra a Figura 5, que apresenta exemplos como (1) a importância da realização de backups, (2) impacto de um phishing e (3) questões relacionadas a vazamento de dados.

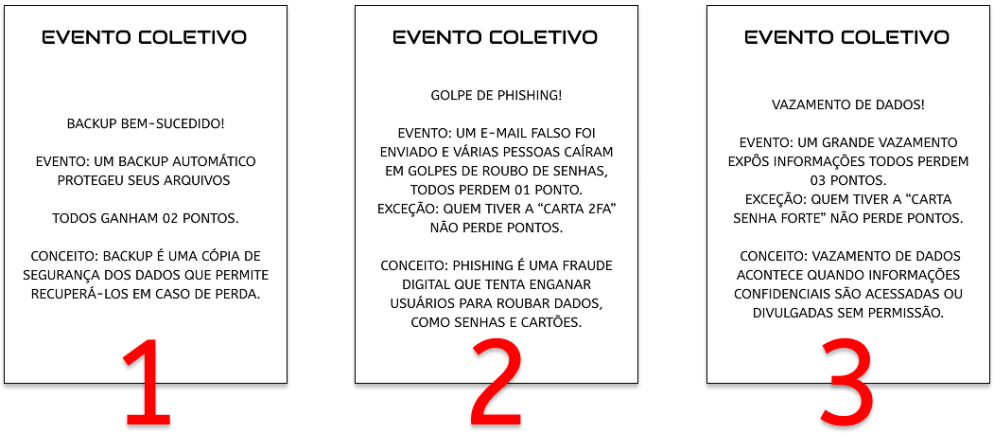


Figura 5: Exemplos de cartas voltadas à prevenção, cooperação e responsabilidade digital.

Por fim, o quarto objetivo (**OE4**) busca desenvolver habilidades de tomada de decisão em situações contextualizadas, exigindo que o estudante avalie alternativas e justifique condutas diante de cenários associados a mensagens suspeitas, arquivos desconhecidos e links recebidos em aplicativos, conforme exemplificado na Figura 6, que ilustra exemplos como: (1) responder uma atitude quanto a links de promoção, (2) atitude sobre arquivos recebidos de colegas desconhecidos e o exemplo (3) sobre links enviados através de aplicativos de mensagem instantânea.

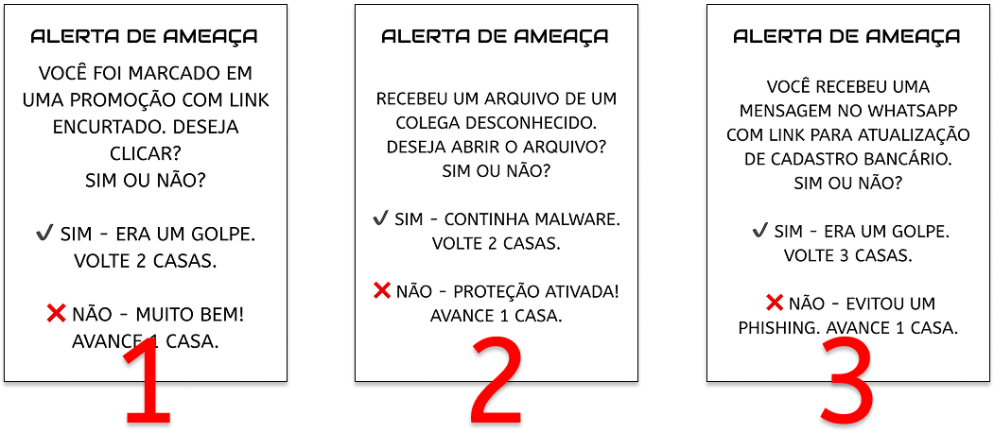


Figura 6: Exemplos de cartas voltadas ao desenvolvimento da tomada de decisão.

4.2 Mecânicas, dinâmica e pontuação

A dinâmica do *CyberQuest* combina movimentação por dado, retirada de cartas, interpretação de situações-problema e gerenciamento de pontos de segurança. Cada jogador inicia a partida com 10 pontos, podendo ganhar ou perder pontuação conforme suas decisões e os eventos enfrentados ao longo do percurso. A Figura 7 apresenta a ficha de pontuação utilizada para o acompanhamento da partida.



CyberQuest

Ficha de Controle de Segurança da Conta

Cada jogador inicia com 10 pontos de segurança.
Use esta ficha para registrar os ganhos e perdas durante a partida.
O vencedor será o jogador com o maior total ao final do jogo.

Rodada	Ganhos(+)	Perdas(-)
	Total	

Figura 7: Ficha de pontuação utilizada pelos jogadores durante a partida.

Embora exista um elemento competitivo associado à pontuação final, a experiência do jogo não se restringe à competição individual. Muitas situações exigem debate entre os participantes, interpretação compartilhada das cartas e negociação em torno de possíveis respostas. Dessa forma, a dinâmica combina competição e colaboração, criando um ambiente em que a aprendizagem emerge da ação individual, mas também das interações sociais estabelecidas durante a partida.

4.3 Componentes, tabuleiro e mediação pedagógica

Os componentes do *CyberQuest* incluem tabuleiro, cartas temáticas, dado e ficha de pontuação. O tabuleiro foi organizado em 100 casas distribuídas em quatro blocos de progressão pedagógica, buscando equilibrar momentos de introdução, intensificação dos desafios, clímax e recuperação. A Figura 8 apresenta a versão utilizada na aplicação do ciclo 2 de validação.

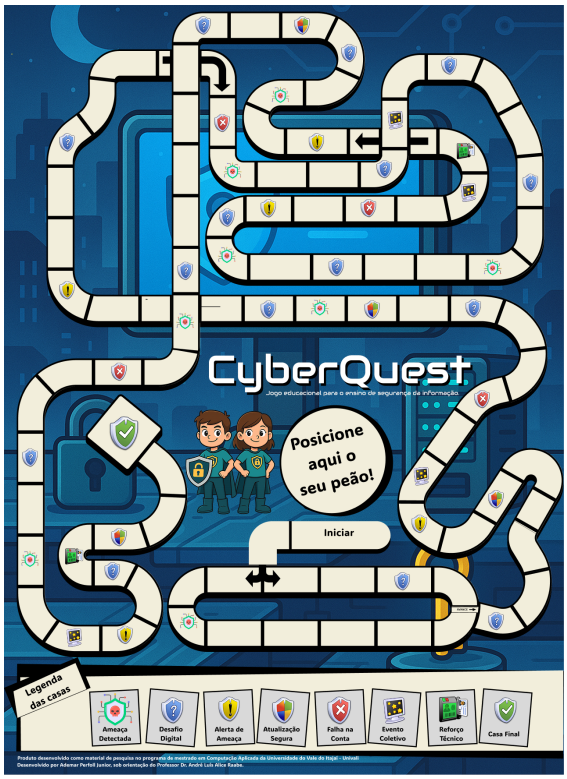


Figura 8: Tabuleiro do *CyberQuest*.

A Figura 9 ilustra exemplos de cartas do jogo, que constituem o núcleo pedagógico da proposta. É sobretudo por meio dessas cartas que o estudante entra em contato com situações de risco, conceitos de segurança e dilemas associados ao uso de tecnologias digitais.



Figura 9: Exemplos de cartas do *CyberQuest*.

A organização do tabuleiro em blocos progressivos busca estruturar uma experiência que

alterna momentos de aprendizagem conceitual, tensão, tomada de decisão e recuperação estratégica. A Figura 10 ilustra essa estrutura, na qual o tabuleiro está organizado em quatro blocos numerados que estruturam a experiência do jogador:

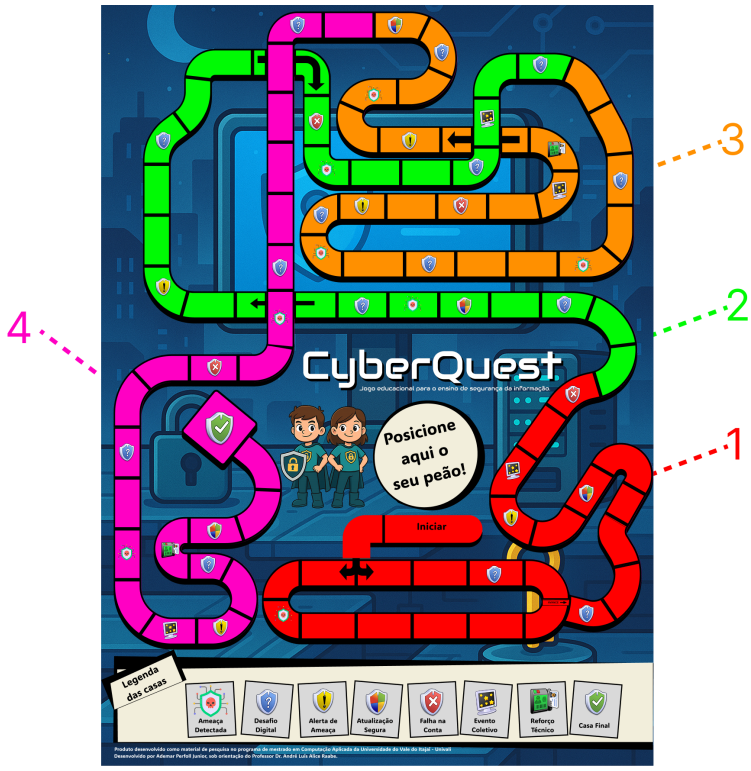


Figura 10: Tabuleiro do *CyberQuest* estruturado em quatro blocos de progressão pedagógica.

Fonte: elaboração própria (autoria suprimida para avaliação às cegas).

A seguir, descreve-se cada um dos quatro blocos de progressão pedagógica:

Bloco (1) identificado pela cor vermelha, corresponde à introdução e ambientação (Casas 1–25), no qual caracteriza-se por ações simples e educativas, com predominância de Casas Normais, Desafios Digitais e Atualizações Seguras. O objetivo é familiarizar o jogador com a mecânica do jogo e com conceitos introdutórios de segurança da informação conforme as cartas retiradas, contribuindo especialmente para o desenvolvimento do **OE2**.

Bloco (2) identificado pela cor verde, corresponde a crescimento e tensão (Casas 26–50), que introduz riscos e situações mais desafiadoras, com aumento gradual de Ameaças Detectadas e Alertas de Ameaça. Essa fase simula incidentes comuns do ambiente digital e estimula a percepção da importância de estratégias preventivas e da coordenação em grupo, mobilizando os objetivos **OE1**, **OE3** e **OE4**.

Bloco (3) identificado pela cor laranja, corresponde ao clímax e riscos (Casas 51–75), onde concentra desafios mais complexos, ameaças recorrentes e penalidades mais severas, exigindo maior atenção, domínio das regras e tomada de decisão consciente. O posicionamento desse trecho como o de maior risco digital reforça principalmente os objetivos **OE1** e **OE4**.

Bloco (4) identificado pela cor rosa, identifica a fase de recuperação e vitória (Casas 76–100),

onde enfatiza o caráter formativo e cooperativo do jogo, incorporando Reforços Técnicos, Atualizações Seguras e Eventos Coletivos que promovem reflexão, retomada de conceitos e aprendizagem colaborativa. A jornada culmina na Casa 100, simbolizando a "Conta Segura Conquistada", associada diretamente ao **OE3**.

Essa organização do tabuleiro foi projetada para garantir dificuldade progressiva e coerência pedagógica, intercalando momentos de aprendizagem conceitual, exposição a riscos e recuperação estratégica. Do ponto de vista educacional, o tabuleiro atua como mediador cognitivo, estimulando raciocínio, tomada de decisão e pensamento estratégico em contextos simulados de uso da tecnologia, em alinhamento direto aos objetivos educacionais **OE1–OE4**.

A mediação pedagógica desempenha função central na utilização do jogo. Cabe ao professor esclarecer regras, organizar a dinâmica da partida e transformar episódios lúdicos em oportunidades de reflexão didática. Desse modo, o *CyberQuest* não opera apenas como atividade recreativa, mas como produto educacional orientado à promoção de argumentação, problematização e reflexão crítica sobre segurança da informação.

5 Método

O estudo foi desenvolvido com base na abordagem *Design-Based Research* (DBR), adotada por sua adequação à investigação de produtos educacionais em contextos autênticos de uso. Conforme Wang e Hannafin (2005), Amiel e Reeves (2008) e Edelson (2002), a DBR permite articular elaboração de artefatos, aplicação em ambientes reais e análise sistemática dos resultados produzidos na interação entre proposta pedagógica, participantes e contexto.

Coerentemente com a natureza iterativa da DBR, a pesquisa que originou o *CyberQuest* foi organizada em ciclos sucessivos de análise, design, implementação e redesenho. O **Ciclo 1 (microfase exploratória)** consistiu na aplicação de um jogo de tabuleiro analógico de temática geral da computação, conduzida pelo pesquisador com o objetivo de testar a viabilidade metodológica do uso de jogos analógicos em sala de aula e validar os instrumentos de coleta de dados, dele resultando princípios de design estruturais (por exemplo, viabilidade do formato analógico, calibração de tempo e complexidade de regras). O **Ciclo 2 (design e avaliação da versão 1.0 do *CyberQuest*)**, foco deste artigo, compreendeu a concepção do jogo a partir dos objetivos educacionais (OE1–OE4) e sua aplicação com 68 estudantes de duas escolas, acompanhada de observação participante, questionário de perfil e grupo focal, com o objetivo de produzir evidências sobre engajamento, indícios de aprendizagem e adequação do design. As evidências obtidas neste ciclo orientam o **Ciclo 3 (refinamento e avaliação da versão 2.0)**, que extrapola o escopo deste artigo e é tratado em trabalho específico, aqui, ele é mencionado apenas como desdobramento futuro. A Figura 11 sintetiza a organização dos ciclos e situa o recorte abordado neste trabalho.

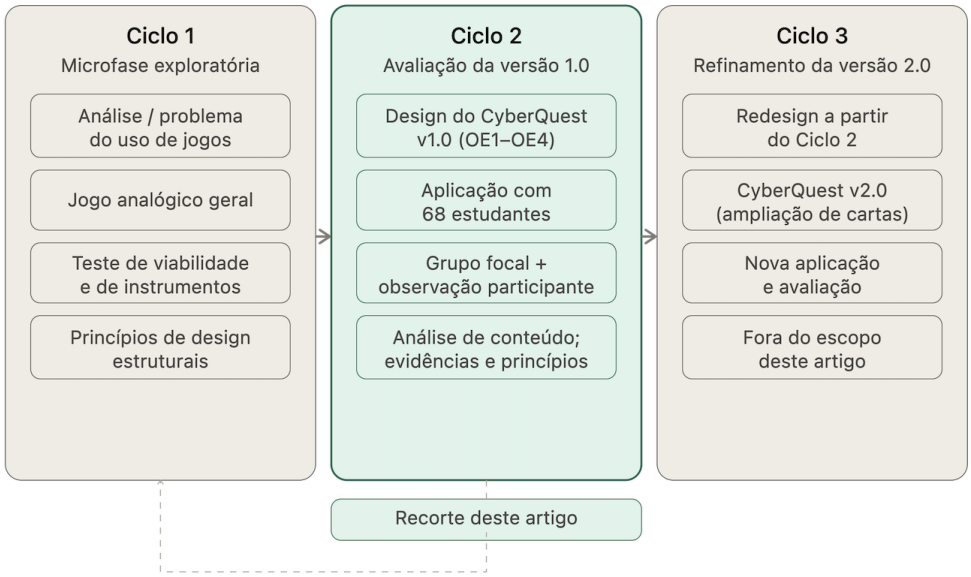


Figura 11: Fases iterativas: análise · design · implementação · análise/redesign.

Neste trabalho, a DBR orientou a investigação dos resultados da avaliação da versão 1.0 do *CyberQuest* (Ciclo 2), focalizando o comportamento dos estudantes durante o uso do jogo, os indícios de aprendizagem emergentes e os aspectos do design que influenciaram a experiência pedagógica.

5.1 Contexto, participantes e aspectos éticos

A investigação foi realizada em duas escolas (omitido para revisão), com participação de 68 estudantes do ensino médio, com idades entre 14 e 18 anos. A participação foi voluntária, com tratamento anônimo dos dados produzidos e observância das orientações institucionais das escolas envolvidas. O projeto está aprovado pelo Comitê de Ética através do Parecer 7.954.798.

5.2 Instrumentos de produção de dados

A produção de dados combinou observação participante, questionário de perfil e grupo focal. A observação participante permitiu registrar aspectos da dinâmica do jogo, como fluidez da partida, dúvidas recorrentes, padrões de interação e episódios de discussão conceitual. O questionário de perfil foi utilizado para caracterizar a experiência prévia dos estudantes em relação ao uso de internet, jogos e temas associados à segurança digital. O grupo focal, por sua vez, foi conduzido ao final das sessões para aprofundar percepções sobre engajamento, aprendizagem percebida e adequação do design do jogo. O Quadro 1 apresenta a síntese dos instrumentos de produção de dados e seus focos de análise.

Quadro 1: Síntese dos instrumentos de produção de dados e seus focos de análise

Instrumento	**Foco de análise**	**Produto gerado**
Observação participante	Fluidez da partida; dúvidas; interação; episódios conceituais	Notas de campo e registros de ocorrência
Questionário de perfil	Uso de internet; familiaridade com jogos; percepção inicial sobre segurança	Caracterização do grupo participante
Grupo focal	Percepções sobre o jogo; aprendizagem percebida; sugestões de melhoria	Excertos discursivos e síntese por categorias analíticas

5.3 Grupo focal

O grupo focal foi realizado imediatamente após as partidas, com duração aproximada de 15 a 20 minutos por turma. O roteiro semiestruturado foi organizado em três eixos: (i) experiência de uso do jogo; (ii) aprendizagens percebidas ao longo da atividade; e (iii) avaliação do design e dos componentes. A condução buscou estimular os estudantes a recuperar episódios concretos da partida, descrevendo situações marcantes, decisões tomadas, dificuldades enfrentadas e conteúdos de segurança mobilizados no decorrer do jogo. Para preservar o anonimato dos participantes, as falas apresentadas na seção de resultados são identificadas pelo código GF seguido de um número (por exemplo, GF17), indicando o estudante participante do grupo focal.

5.3.1 Roteiro do grupo focal e questionário de perfil

A condução do grupo focal no Ciclo 2 da aplicação do *CyberQuest* (avaliação da versão 1.0) foi orientada por um roteiro semiestruturado elaborado para investigar percepções dos estudantes sobre a experiência de jogar, os indícios de aprendizagem percebida, a relação entre o jogo e situações do cotidiano digital, bem como aspectos de engajamento, clareza das regras e possibilidades de melhoria do produto educacional. O roteiro foi composto por dez perguntas abertas, apresentados no Quadro 2.

Além do grupo focal, foi aplicado um questionário de perfil com o objetivo de caracterizar os participantes quanto à idade, série escolar, experiência prévia com jogos de tabuleiro educativos, uso da internet, familiaridade com o tema segurança da informação e eventual vivência de problemas relacionados à segurança no ambiente digital. As perguntas desse instrumento estão apresentadas no Quadro 3.

Quadro 2: Perguntas de abordagem do grupo focal (roteiro)

N.	Pergunta
P1	Alguém já tinha jogado algum jogo de tabuleiro educativo antes? Como foi?
P2	Como vocês se sentiram ao jogar o CyberQuest? (momentos marcantes, participação individual e em grupo)
P3	Vocês acham que aprenderam algo sobre segurança da informação jogando o CyberQuest? O quê?
P4	O jogo lembrou vocês de algo vivido por vocês ou por alguém próximo na internet?
P5	O jogo manteve a atenção até o final? O que ajudou ou atrapalhou?
P6	Jogar em grupo foi mais interessante do que apenas ler sobre o conteúdo? Por quê?
P7	Se pudessem mudar algo no jogo, o que seria?
P8	O jogo poderia ser usado em outras turmas? Por quê?
P9	As regras foram fáceis de entender? Surgiram dúvidas durante a partida?
P10	Alguma parte pareceu difícil ou confusa? Como poderia ser melhor?

Quadro 3: Perguntas do questionário de perfil dos participantes

N.	Pergunta
P1	Idade
P2	Ano/Série em que está matriculado(a)
P3	Já jogou algum jogo de tabuleiro educativo antes?
P4	(Se sim) Em qual disciplina/matéria?
P5	Com que frequência utiliza a internet?
P6	Já ouviu falar em segurança da informação?
P7	(Se sim) O que entende por segurança da informação?
P8	Já teve algum problema com segurança na internet? (golpes, invasões, vazamentos)

As perguntas do grupo focal foram utilizadas como guia para a mediação das discussões, permitindo explorar tanto percepções espontâneas dos estudantes quanto aspectos diretamente relacionados aos objetivos do estudo. Já o questionário de perfil contribuiu para contextualizar as falas dos participantes e apoiar a interpretação dos dados qualitativos produzidos durante a aplicação do jogo.

5.4 Procedimentos de análise dos dados

Os dados foram analisados qualitativamente, com triangulação entre observação participante, questionário de perfil e grupo focal. A análise das falas seguiu a técnica de Análise de Conteúdo (Bardin, 2011), conduzida nas três etapas propostas pela autora: (i) pré-análise, com a transcrição e a leitura flutuante dos registros do grupo focal e das notas de campo; (ii) exploração do material, com a codificação de trechos significativos e seu agrupamento em categorias; e (iii) tratamento e interpretação dos resultados. A categorização foi conduzida de forma predominantemente indutiva, com as categorias emergindo das falas dos próprios participantes, em diálogo com os eixos do roteiro e com os objetivos educacionais do jogo (OE1–OE4). Desse processo resultaram três categorias analíticas: (i) engajamento e dinâmica social; (ii) aprendizagem situada e compreensão conceitual; e (iii) adequação do design do jogo. As categorias foram estabilizadas pela convergência entre os temas recorrentes nas falas dos estudantes, os episódios observados durante a aplicação e os objetivos pedagógicos do jogo. As falas dos estudantes foram interpretadas em articulação com os episódios observados durante a aplicação, buscando compreender não apenas o que os participantes relataram, mas também como essas percepções se manifestaram na experiência concreta de uso do *CyberQuest*.

5.5 Procedimentos de aplicação

A aplicação ocorreu em sessões presenciais com duração aproximada de 45 a 60 minutos, organizadas em três momentos: (i) apresentação do objetivo do jogo, da narrativa e das regras; (ii) realização da partida em grupos; e (iii) condução do grupo focal ao final da atividade. Durante as sessões, o pesquisador realizou mediação contínua, especialmente em situações de dúvida sobre regras, uso de cartas e registro de pontuação, além de estimular a explicitação de raciocínios sempre que surgiam decisões relacionadas a riscos digitais. A Figura 12 apresenta um momento da

mediação realizada durante a aplicação.



Figura 12: Mediação do pesquisador durante a aplicação do jogo.

6 Resultados e Discussão

Esta seção apresenta os resultados obtidos a partir da aplicação do CyberQuest nas duas escolas participantes do estudo. A análise dos dados provenientes do grupo focal foi realizada por meio de categorização temática das falas dos estudantes, considerando as dimensões investigadas no roteiro de perguntas apresentado na Seção de Métodos. As perguntas do grupo focal exploraram percepções sobre a experiência de jogar o *CyberQuest*, indícios de aprendizagem percebida, relação entre o jogo e situações vivenciadas no ambiente digital, manutenção da atenção ao longo da atividade e avaliação do design do jogo.

A partir da análise das respostas às perguntas P1–P10, e seguindo o procedimento de Análise de Conteúdo descrito na Seção de Método, os dados foram organizados em três categorias analíticas principais: (i) engajamento e dinâmica social; (ii) aprendizagem situada e compreensão conceitual; e (iii) adequação do design do jogo. Essas categorias resultaram da convergência entre os temas recorrentes nas falas dos estudantes, os episódios registrados na observação participante e os objetivos pedagógicos do jogo.

6.1 Engajamento e dinâmica social

As perguntas relacionadas à experiência de uso do jogo (P2, P5 e P6) permitiram compreender como os estudantes perceberam a dinâmica da atividade e a interação entre os participantes durante as partidas. De modo geral, os relatos indicam elevado nível de engajamento dos estudantes,

associado principalmente à interação social, ao caráter competitivo da atividade e à dinâmica coletiva proporcionada pelo jogo.

Durante a aplicação, observou-se que os estudantes acompanharam atentamente as jogadas dos colegas e frequentemente participaram das decisões, mesmo quando não era sua vez de jogar. A resolução das situações apresentadas nas cartas frequentemente mobilizou discussões coletivas, nas quais os participantes sugeriam respostas, comentavam experiências pessoais relacionadas ao uso da internet e avaliavam as decisões tomadas pelos colegas.

As falas do grupo focal reforçam essa percepção ao destacar o caráter interativo da atividade. Um estudante afirmou:

"Foi bem dinâmico e interativo, todos os momentos deram risadas incríveis." (GF17)

Outro participante ressaltou o papel da interação social na experiência de jogo:

"Foi divertido jogar com meus amigos, todos participaram e o jogo funciona." (GF15)

A competitividade também apareceu como elemento importante para manter o interesse dos participantes ao longo da atividade. Em resposta à pergunta sobre o que ajudou a manter a atenção durante o jogo (P5), alguns estudantes destacaram diretamente o aspecto competitivo da dinâmica:

"O que ajudou foi a sede de ganhar." (GF2)

"Sim, a competitividade." (GF39)

Além disso, alguns elementos específicos do jogo, como os eventos coletivos, foram citados como momentos particularmente marcantes da experiência lúdica:

"A parte que eu mais gostei foi quando pegávamos o evento coletivo." (GF22)

Esses registros indicam que o engajamento observado não se restringe ao caráter divertido da atividade, mas está associado à dinâmica social promovida pelo jogo. A circulação de falas, a negociação de respostas e a interação entre os participantes contribuíram para transformar a atividade em um espaço coletivo de participação e discussão. Em termos de Informática na Educação, esse resultado reforça o potencial de jogos de tabuleiro como tecnologias educacionais capazes de promover interação social significativa em contextos escolares, convergindo com evidências reportadas em estudos sobre jogos educacionais analógicos (González-Tablas et al., 2020; Stsiampkouskaya et al., 2025).

6.2 Aprendizagem situada e compreensão conceitual

As perguntas relacionadas à aprendizagem percebida e à relação entre o jogo e experiências do cotidiano digital (P3 e P4) permitiram investigar de que forma os estudantes compreenderam os conteúdos de segurança da informação apresentados durante a atividade.

De modo geral, os relatos indicam que os estudantes perceberam o jogo como uma oportunidade de discutir situações reais relacionadas ao uso da internet e das redes sociais. Em diversas mesas, a resolução das cartas levou os participantes a compartilhar experiências pessoais envolvendo golpes digitais, mensagens suspeitas ou práticas de segurança na utilização de aplicativos e plataformas online.

Esse aspecto aparece de forma clara em alguns relatos registrados no grupo focal. Um participante destacou que a atividade estimulou a troca de experiências entre os colegas:

> "A interação com os outros foi boa, contaram alguns relatos que tiveram com o uso da internet e rimos bastante." (GF26)

Outro estudante destacou que a aprendizagem ocorreu justamente a partir das discussões entre os participantes:

> "Foi mais legal pois você discute com seus amigos e aprende com eles também." (GF3)

Em direção semelhante, outro participante afirmou:

> "Jogar com outras pessoas é mais legal porque está todo mundo interessado, e cada um vai aprendendo junto." (GF10)

Esses relatos indicam que o *CyberQuest* favoreceu uma forma de aprendizagem situada, na qual os conceitos de segurança da informação foram mobilizados em situações concretas de decisão. Em vez de serem apresentados apenas como conteúdos informativos, temas como *phishing*, privacidade e proteção de dados apareceram vinculados a cenários que exigiam interpretação, escolha e justificativa.

Além da mobilização conceitual, observaram-se episódios em que a atividade favoreceu a reflexão crítica dos estudantes sobre suas próprias práticas digitais. Durante a resolução de cartas associadas a ameaças e mensagens suspeitas, foram registrados na observação participante momentos em que os participantes relacionaram os conteúdos do jogo a vivências pessoais e familiares, mencionando situações como reutilização de senhas, links suspeitos, golpes ocorridos com familiares e aceitação indiscriminada de *cookies*. Essa aproximação entre o jogo e o cotidiano também aparece nas falas registradas no grupo focal, como na de um estudante que sintetizou a aprendizagem adquirida:

> "Aprendi sobre *phishing* e *malware*, termos que eu não conhecia."

Episódios como esses evidenciam que a reflexão não permaneceu apenas no plano conceitual, mas se traduziu na revisão de atitudes e na explicitação de critérios para decisões mais seguras, a partir do reconhecimento de riscos antes naturalizados. A mediação pedagógica teve papel central nesse processo, ao instigar os estudantes a justificar suas escolhas e a confrontar diferentes pontos de vista durante as discussões, transformando situações do jogo em oportunidades de problematização do cotidiano digital.

Esse resultado é particularmente relevante para o contexto da educação básica, pois aproxima o ensino de segurança digital das experiências cotidianas dos estudantes no ambiente online. Ao discutir problemas concretos relacionados ao uso da internet, o jogo contribui para o desenvolvimento de competências associadas à cidadania digital e ao uso crítico das tecnologias.

6.3 Adequação do design do jogo

As perguntas relacionadas à avaliação do jogo (P7, P8, P9 e P10) permitiram identificar percepções dos estudantes sobre o design, a clareza das regras e possíveis melhorias para a experiência de uso do *CyberQuest*.

De modo geral, os estudantes avaliaram positivamente a dinâmica do jogo e o ritmo das partidas. Alguns participantes destacaram que a estrutura da atividade contribuiu para manter a atenção ao longo da experiência:

> "Foi uma experiência divertida e rápida." (GF19)

> "A dinâmica rápida ajudou a manter a atenção." (GF40)

Entretanto, alguns estudantes também apontaram limitações relacionadas à repetição de cartas e à variedade dos desafios apresentados durante o jogo. Em alguns relatos, os participantes mencionaram que a repetição de perguntas pode ter influenciado a percepção de cansaço nas rodadas finais:

> "No início estava interessado, mas ao decorrer do jogo achei ele repetitivo demais." (GF21)

> "O final ficou muito cansativo pois as perguntas e desafios se repetiam." (GF24)

Essas observações não comprometem a viabilidade pedagógica da atividade, mas indicam oportunidades de refinamento no design do jogo. A ampliação do banco de cartas e a diversificação dos desafios podem contribuir para manter o equilíbrio entre novidade, desafio e engajamento ao longo das partidas. Em coerência com a lógica iterativa da DBR, as sugestões e observações fornecidas pelos estudantes durante o grupo focal foram sistematizadas e incorporadas ao planejamento de uma versão revisada do *CyberQuest* (versão 2.0), correspondente ao Ciclo 3 da pesquisa, que contempla, sobretudo, a ampliação e a diversificação do conjunto de cartas. Essa versão refinada, por extrapolar o escopo deste artigo, é objeto de trabalho específico. O Quadro 4 apresenta a organização das categorias, evidências, falas e implicações educacionais resultantes da análise da pesquisa.

Quadro 4: Aplicação do *CyberQuest*: categorias, evidências, falas e implicações educacionais.

Categoria	**Perguntas associadas**	**Excerto do grupo focal**	**Interpretação analítica**	**Implicações educacionais**
Engajamento e dinâmica social	P2, P5, P6	"Foi bem dinâmico e interativo, todos os momentos deram risadas incríveis." (GF17)	A interação social e a competitividade contribuíram para a manutenção do interesse dos estudantes durante as partidas.	Jogos de tabuleiro podem promover participação ativa e interação presencial em contextos educacionais.
Aprendizagem situada e compreensão conceitual	P3, P4	"Foi mais legal pois você discute com seus amigos e aprende com eles também." (GF3)	Os conceitos de segurança digital foram mobilizados em contextos de decisão relacionados a experiências reais dos estudantes.	Jogos educacionais podem aproximar conteúdos escolares das experiências digitais cotidianas dos alunos.
Adequação do design do jogo	P7, P8, P9, P10	"No início estava interessado, mas ao decorrer do jogo achei ele repetitivo demais." (GF21)	A diversidade das cartas e a clareza das regras influenciam a manutenção do engajamento ao longo da partida.	Refinamentos no design do jogo podem ampliar seu potencial pedagógico e melhorar a experiência de uso.

Os resultados indicam que o valor pedagógico do *CyberQuest* emerge da integração entre interação social, mobilização conceitual e estrutura lúdica. O engajamento observado nas partidas está diretamente relacionado à dinâmica coletiva promovida pelo jogo, enquanto os episódios de aprendizagem surgem principalmente nas discussões em torno das decisões apresentadas nas cartas. Ao mesmo tempo, a análise das percepções dos estudantes permite identificar oportunidades de refinamento no design do jogo, especialmente no que se refere à diversidade dos desafios e à evolução das situações apresentadas durante as partidas.

6.4 Limitações e ameaças à validade

A discussão das limitações deste estudo requer, preliminarmente, o reconhecimento de que a escolha pela DBR implica um entendimento particular de validade. Toda pesquisa enfrenta uma tensão

inerente entre a validade interna, associada ao controle de variáveis em ambientes de laboratório, e a validade ecológica, associada à aplicabilidade dos resultados no mundo real (Barab & Squire, 2004). Essas duas dimensões dificilmente são maximizadas ao mesmo tempo (Palmér & Van Bommel, 2021): ao mover a investigação para a sala de aula real e tratar as dinâmicas sociais, as restrições de tempo e a infraestrutura escolar como parte do fenômeno estudado, a DBR abre mão deliberadamente de parte do controle laboratorial para assegurar que a intervenção efetivamente funcione no contexto em que será utilizada (Scott et al., 2020). Sob essa perspectiva, algumas limitações apontadas a seguir não representam falhas do desenho, mas decorrem, de forma inerente e assumida, da priorização da validade ecológica própria da abordagem.

Quanto à **validade interna**, o caráter qualitativo e situado da investigação, somado à atuação do pesquisador também como mediador e observador participante, pode introduzir vieses de interpretação e de desejabilidade social nas respostas dos estudantes. Coerentemente com a lógica da DBR, esse risco é mitigado não pela eliminação de variáveis, mas pela triangulação de múltiplas fontes de dados e pela iteração ao longo dos ciclos (Kennedy-Clark, 2013). No que se refere às **evidências de aprendizagem**, o estudo apoia-se em aprendizagem percebida e em indícios observados durante a aplicação, não tendo sido empregado instrumento de avaliação de desempenho (pré e pós-teste); trata-se, portanto, de indícios e não de comprovação de ganhos conceituais. Quanto à **validade externa**, reconhece-se a tensão, própria da DBR, entre o refinamento local da prática e a generalização ampla (Scott et al., 2020): os resultados decorrem da aplicação em duas escolas, com 68 estudantes, em um único ciclo de avaliação da versão 1.0 (Ciclo 2), de modo que sua contribuição não reside na generalização estatística, mas na produção de princípios de design transferíveis a outros contextos. Por fim, como ameaça de **construto**, reconhece-se que conceitos como engajamento e reflexão crítica foram inferidos a partir de falas e comportamentos, o que demanda cautela interpretativa. Essas limitações orientam os próximos ciclos da pesquisa, que preveem a incorporação de instrumentos complementares de avaliação e a ampliação dos contextos de aplicação.

7 Conclusões

Este artigo investigou os resultados da aplicação do jogo de tabuleiro *CyberQuest* como produto educacional voltado ao ensino de segurança da informação no ensino médio. A análise dos dados produzidos com 68 estudantes de duas escolas (omitido para revisão) evidenciou que o jogo favoreceu alto engajamento, intensa participação social e mobilização de conhecimentos relacionados à segurança digital em situações contextualizadas.

Os resultados indicam que o *CyberQuest* operou como uma tecnologia educacional analógica capaz de articular ludicidade, mediação pedagógica e reflexão crítica. Mais do que despertar interesse pelo tema, o jogo criou condições para que os estudantes discutissem riscos, comparassem alternativas de ação, justificassem decisões e relacionassem os conteúdos abordados às próprias experiências no ambiente digital. Nesse sentido, a principal contribuição do estudo não está apenas na existência de um jogo sobre segurança da informação, mas na demonstração de que a aplicação desse artefato em contexto escolar pode favorecer formas qualificadas de participação e elaboração conceitual.

O trabalho contribui ao demonstrar que jogos de tabuleiro podem constituir recursos consis-

tentes para tratar temas contemporâneos e socialmente relevantes no ensino médio, especialmente quando articulados à mediação pedagógica e à problematização de situações próximas da realidade dos estudantes. A investigação também evidenciou que a qualidade da experiência educacional depende não apenas do conteúdo abordado, mas do modo como o jogo estrutura interação, progressão, clareza de regras e legibilidade dos componentes.

Por fim, os resultados também tornaram visíveis aspectos do design que influenciam diretamente o uso pedagógico do *CyberQuest*, como variedade das cartas, clareza instrucional e organização visual dos materiais. Esses elementos não reduzem a consistência do produto educacional, ao contrário, qualificam sua análise ao evidenciar dimensões concretas que afetam a experiência dos estudantes em contexto real de aplicação. Assim, o estudo reforça o potencial dos jogos de tabuleiro como tecnologias educacionais para a promoção da cidadania digital e para o ensino de segurança da informação na educação básica.

Referências

Amiel, T., & Reeves, T. C. (2008). Design-based research and educational technology: Rethinking technology and the role of theory in practice. *Educational Technology & Society*, *11*(4), 29–40. [GS Search].

Barab, S., & Squire, K. (2004). Design-Based Research: Putting a Stake in the Ground. *Journal of the Learning Sciences*, *13*(1), 1–14. https://doi.org/10.1207/s15327809jls1301_1 [GS Search].

Bardin, L. (2011). *Análise de Conteúdo*. Edições 70. [GS Search].

Brasil. (2018). Base Nacional Comum Curricular [Versão homologada]. http://basenacionalcomum.mec.gov.br/ [GS Search].

Brasil. (2022). Normas sobre Computação na Educação Básica – Complemento à BNCC [Parecer CNE/CP nº 2/2022. Conselho Nacional de Educação]. http://basenacionalcomum.mec.gov.br/ [GS Search].

Controladoria-Geral da União (CGU) e Universidade Federal de Goiás (UFG). (2023). Game da Cidadania [Recurso educacional. Acesso em: 2026]. https://www.gov.br/cgu/pt-br/educacao-cidada/programas/game-da-cidadania [GS Search].

Edelson, D. C. (2002). Design research: What we learn when we engage in design. *Journal of the Learning Sciences*, *11*(1), 105–121. https://doi.org/10.1207/S15327809JLS1101_4 [GS Search].

Gomes, B. A., & Ulbricht, V. R. (2024). Os jogos de tabuleiro e seu uso na educação: uma revisão integrativa de literatura. *Educação Unisinos*, *28*, 1–18. https://doi.org/10.4013/edu.2024.281.01 [GS Search].

González-Tablas, A. I., González Vasco, M. I., Cascos, I., & Planet Palomino, Á. (2020). Shuffle, Cut, and Learn: Crypto Go, a Card Game for Teaching Cryptography. *Mathematics*, *8*(11), 1993. https://doi.org/10.3390/math8111993 [GS Search].

Instituto Cidadão Digital. (2025). Trilha Cidadão Digital [Iniciativa educacional. Acesso em: 2026]. https://cidadaodigital.org.br/ [GS Search].

Kennedy-Clark, S. (2013). Research by Design: Design-Based Research and the Higher Degree Research Student. *Journal of Learning Design*, *6*(2), 26–32. https://doi.org/10.5204/jld.v6i2.128 [GS Search].

Lave, J., & Wenger, E. (1991). *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press. https://doi.org/10.1017/CBO9780511815355 [GS Search].

Palmér, H., & Van Bommel, J. (2021). Teachers' participation in practice based research – a methodological retrospect. *NOMAD Nordic Studies in Mathematics Education*, *26*(3-4), 87–100. https://doi.org/10.7146/nomad.v26i3-4.149174 [GS Search].

Scott, E. E., Wenderoth, M. P., & Doherty, J. H. (2020). Design-Based Research: A Methodology to Extend and Enrich Biology Education Research. *CBE—Life Sciences Education*, *19*(1), es11. https://doi.org/10.1187/cbe.19-11-0245 [GS Search].

Serpro. (2023). SerDigi: jogo educativo sobre segurança digital [Acesso em: 2026]. https://campanhas.serpro.gov.br/serdigi/ [GS Search].

Silva, T. R. d., Medeiros, T., Medeiros, H., Lopes, R., & Aranha, E. (2015). Ensino-aprendizagem de programação: uma revisão sistemática da literatura. *Revista Brasileira de Informática na Educação (RBIE)*, *23*(1), 182–196. https://doi.org/10.5753/RBIE.2015.23.01.182 [GS Search].

Stsiampkouskaya, K., Kundu, O., Syrda, J., & Joinson, A. (2025). Threats & Trade-offs: A Start-up Simulation Game for Cybersecurity and Innovation Decision-Making. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10604-3 [GS Search].

Wang, F., & Hannafin, M. J. (2005). Design-Based Research and Technology-Enhanced Learning Environments. *Educational Technology Research and Development*, *53*(4), 5–23. https://doi.org/10.1007/BF02504682 [GS Search].