

Aprendizagem Baseada em Jogos: uma abordagem para o ensino de cibersegurança no 9º ano

Title: Game-Based Learning: an approach to teaching cybersecurity in 9th grade

Título: Aprendizaje Basado en Juegos: un enfoque para la Enseñanza de la Ciberseguridad en 9.º Grado

Daniela Barbosa de Sousa
Instituto Federal de Educação, Ciência e Tecnologia
do Pará, campus Castanhal
ORCID: [0009-0007-4604-1472](https://orcid.org/0009-0007-4604-1472)
db085721@gmail.com

Renan Anezio da Rocha
Instituto Federal de Educação, Ciência e Tecnologia
do Pará, campus Castanhal
ORCID: [0009-0006-2164-7411](https://orcid.org/0009-0006-2164-7411)
renan18anezio@gmail.com

Franciel da Silva Amorim
Instituto Federal de Educação, Ciência e Tecnologia
do Pará, campus Castanhal
ORCID: [0009-0005-7219-7302](https://orcid.org/0009-0005-7219-7302)
franciel.amorim@ifpa.edu.br

Andréa Guimarães Ribeiro Ohashi
Instituto Federal de Educação, Ciência e Tecnologia
do Pará, campus Castanhal
ORCID: [0009-0006-7704-3350](https://orcid.org/0009-0006-7704-3350)
andrea.ohashi@ifpa.edu.br

Resumo

A crescente integração de dispositivos digitais no cotidiano de crianças e adolescentes eleva sua exposição a riscos online. Diante do aumento expressivo de ataques cibernéticos e da complexidade inerente aos conceitos de malware e segurança digital, emerge a premente necessidade de investigar e aplicar metodologias dinâmicas e eficazes no âmbito do ensino de cibersegurança. Isso posto, este estudo tem como objetivo investigar o potencial da Aprendizagem Baseada em Jogos (ABJ), especificamente por meio da elaboração e implementação de um jogo de tabuleiro, no ensino de cibersegurança para estudantes do 9º ano do ensino fundamental de uma escola municipal em Castanhal (PA). A partir de uma metodologia quanti-qualitativa (Gil, 2017) e pesquisa aplicada (Gerhardt; Silveira, 2009), o estudo coletou dados mediante questionários pré e pós-intervenção e observação participante (Severino, 2017), complementados por análise de conteúdo (Bardin, 2016), para avaliar o impacto do jogo no conhecimento e na conscientização dos alunos sobre riscos e defesas cibernéticas. Essa intervenção, com 12 estudantes, promoveu um aumento de 40% para 60% na taxa de acertos na compreensão dos conceitos e no engajamento dos alunos. Os resultados evidenciam a eficácia da ABJ como estratégia acessível e relevante para a formação de cidadãos para uma sociedade digital segura, alinhada às diretrizes da Base Nacional Comum Curricular (BNCC).

Palavras-Chave: Cibersegurança; Aprendizagem Baseada em Jogo (ABJ); Base Nacional Comum Curricular (BNCC).

Abstract

The increasing integration of digital devices into the daily lives of children and adolescents heightens their exposure to online risks. In light of the significant rise in cyberattacks and the inherent complexity of concepts such as malware and digital security, there is a pressing need to explore and apply dynamic and effective methodologies in cybersecurity education. In this context, the present study aims to investigate the potential of Game-Based Learning (GBL), specifically through the design and implementation of a board game, for teaching cybersecurity to 9th-grade students at a municipal school in Castanhal (PA), Brazil. Based on a quantitative-qualitative approach (Gil, 2017) and applied research (Gerhardt & Silveira, 2009), data were collected through pre- and post-intervention questionnaires and participant observation (Severino, 2017), complemented by content analysis (Bardin, 2016), to assess the impact of the game on students' knowledge and awareness of cyber risks and defenses. This intervention, involving 12 students, led to an increase in correct answers from 40% to 60% in the understanding of concepts and

Cite as: Sousa, D. B., Rocha R. A., Amorim, F. S., Ohashi, A. G. R. (2026). Aprendizagem Baseada em Jogos: uma Abordagem para o Ensino de Cibersegurança no 9º Ano. Revista Brasileira de Informática na Educação, vol. 34, 865-897. <https://doi.org/10.5753/rbie.2026.6264>

student engagement. The results highlight the effectiveness of GBL as an accessible and relevant strategy for educating citizens for a secure digital society, aligned with the guidelines of the Brazilian National Common Curricular Base (BNCC).

Keywords: Cybersecurity; Game-Based Learning (GBL); National Common Curricular Base (BNCC).

Resumen

La creciente integración de dispositivos digitales en la vida cotidiana de niños y adolescentes aumenta su exposición a riesgos en línea. Ante el significativo aumento de los ciberataques y la complejidad inherente a conceptos como malware y seguridad digital, surge la necesidad urgente de investigar y aplicar metodologías dinámicas y eficaces en la enseñanza de la ciberseguridad. En este contexto, el presente estudio tiene como objetivo investigar el potencial del Aprendizaje Basado en Juegos (ABJ), específicamente a través del diseño e implementación de un juego de mesa, en la enseñanza de la ciberseguridad a estudiantes del 9° grado de una escuela municipal en Castanhal (PA), Brasil. A partir de una metodología cuantitativa-cualitativa (Gil, 2017) y una investigación aplicada (Gerhardt y Silveira, 2009), se recopilaron datos mediante cuestionarios antes y después de la intervención, así como observación participante (Severino, 2017), complementados con análisis de contenido (Bardin, 2016), para evaluar el impacto del juego en el conocimiento y la concienciación de los estudiantes sobre los riesgos y las defensas cibernéticas. Esta intervención, con la participación de 12 estudiantes, promovió un aumento del 40% al 60% en la tasa de aciertos en la comprensión de los conceptos y en el compromiso de los alumnos. Los resultados evidencian la eficacia del ABJ como una estrategia accesible y relevante para la formación de ciudadanos en una sociedad digital segura, en consonancia con las directrices de la Base Nacional Común Curricular (BNCC) de Brasil.

Palabras clave: Ciberseguridad; Aprendizaje Basado en Juegos (ABJ); Base Nacional Común Curricular (BNCC).

1 Introdução

O avanço tecnológico e o crescente uso de dispositivos digitais entre crianças e adolescentes têm transformado as formas de interação, aprendizado e lazer. Conforme a pesquisa TIC Kids Online Brasil¹, realizada pelo Comitê Gestor da Internet no Brasil (2024), 93% dos jovens de 9 a 17 anos no Brasil utilizam a internet, sendo que 26% dos jovens de 11 a 17 anos assumem que não sabem identificar se um site é confiável. Esses dados destacam a ubiquidade das tecnologias digitais no cotidiano juvenil e a necessidade de práticas educativas que promovam um uso seguro e consciente desses recursos.

Contudo, o cenário da cibersegurança apresenta desafios crescentes. A Check Point Research (2024)² relatou um aumento de 30% nos ataques cibernéticos globais, com a América Latina sendo uma das regiões mais afetadas (+53%), o que reflete a vulnerabilidade das redes e dispositivos digitais. No Brasil, ataques a dispositivos móveis são particularmente alarmantes, posicionando o país no topo da lista dos que mais sofrem ameaças na América Latina (Kaspersky, 2023).

No âmbito escolar, a pesquisa TIC Educação, realizada pelo Núcleo de Informação e Coordenação do Ponto BR – NIC.br. (2024)³, aponta que 56% dos estudantes que utilizam internet buscam nos professores informações sobre o uso de tecnologias digitais, o que reforça a necessidade de metodologias que trabalhem essa temática de forma sistemática e eficaz. Em relação à cibersegurança, o complemento à computação da Base Nacional Comum Curricular (BNCC), publicada em 2022 pelo Ministério da Educação, enfatiza a importância de desenvolver competências digitais que permitam aos estudantes compreender, analisar e utilizar tecnologias de maneira ética e segura.

Nesse contexto, a Aprendizagem Baseada em Jogos (ABJ) surge como uma abordagem promissora para o ensino de cibersegurança, especialmente no 9º ano do ensino fundamental, nível no qual o complemento à Computação da BNCC (Brasil, 2022) estabelece, no eixo Mundo Digital, a introdução de conteúdos específicos sobre Segurança Cibernética nesse nível de ensino. Entre as habilidades previstas, destaca-se a compreensão do funcionamento de malwares e outros tipos de ataques, além do desenvolvimento de atitudes éticas e responsáveis no uso das tecnologias.

Ao proporcionar uma experiência educacional prática, colaborativa e dinâmica, os jogos podem facilitar a assimilação e internalização de conhecimentos de forma significativa e relevante. Essa estratégia pode capacitar estudantes do 9º ano do ensino fundamental a compreenderem os riscos dos ambientes digitais de maneira crítica e autônoma, e a identificar e adotar técnicas de segurança para prevenir os principais ataques cibernéticos, como ransomware, phishing, trojan, entre outros.

Com base nessas premissas, questiona-se: como a ABJ pode contribuir para o ensino e conscientização da cibersegurança entre estudantes do 9º ano do ensino fundamental? Para tanto, o presente estudo tem como objetivos avaliar a ABJ no ensino e conscientização sobre cibersegurança; elaborar e implementar um jogo de tabuleiro para representar as principais ameaças cibernéticas e técnicas de defesa em uma turma do 9º ano do ensino fundamental; e avaliar o conhecimento dos estudantes dessa turma em relação à cibersegurança, antes e após a aplicação do jogo.

¹ Disponível em: [Cetic.br - TIC Kids Online Brasil](https://cetic.br/tic-kids-online-brasil/).

² Disponível em: <https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/>.

³ Disponível em: [tic_educacao_2024_livro_eletronico.pdf](https://nic.br/tic-educacao-2024-livro-eletronico.pdf).

Este artigo está organizado em oito seções principais: a Seção 2 apresenta uma introdução à segurança da informação e à cibersegurança. A Seção 3 aborda as metodologias ativas. Na Seção 4, descreve-se a metodologia da pesquisa, e a Seção 5 reúne os trabalhos relacionados ao tema. A Seção 6 detalha a concepção do jogo Hacker-Ataque, enquanto a Seção 7 discute a análise dos resultados. Por fim, a Seção 8 traz as considerações finais do estudo, seguidas pelas referências.

2 Segurança da Informação e Cibersegurança

A Segurança da Informação (SI) é uma área de conhecimento que visa garantir a proteção de dados em diversos contextos, sejam eles organizacionais (públicos e privados) ou pessoais. Conforme a norma ISO/IEC 27001 (ABNT, 2013), a efetividade da SI fundamenta-se em três princípios basilares: confidencialidade, integridade e disponibilidade (conhecidos pelo acrônimo CID). A confidencialidade assegura que as informações sejam acessadas apenas por indivíduos autorizados; a integridade protege os dados contra modificações não autorizadas; e a disponibilidade garante que os dados estejam acessíveis sempre que necessário.

Embora a SI e Cibersegurança sejam áreas interligadas que buscam proteger dados e sistemas, elas possuem focos distintos. Enquanto a SI abrange a proteção de informações em geral (digitais e físicas), a cibersegurança, ou segurança cibernética, concentra-se especificamente na proteção de ativos digitais, como redes, sistemas, dispositivos e serviços conectados, contra ameaças oriundas do ambiente cibernético. Com a crescente expansão das atividades online e a interconexão de dispositivos, a cibersegurança tornou-se um componente essencial e indissociável da SI, englobando tanto a implementação de medidas tecnológicas de proteção quanto a indispensável conscientização dos usuários sobre práticas seguras na internet (Barros, 2023).

A educação em SI e cibersegurança exerce um papel crucial na preparação dos indivíduos para enfrentar os desafios relacionados à segurança. Sua implementação vai além de informar sobre ameaças cibernéticas, promovendo também o desenvolvimento de habilidades para identificar, prevenir, gerenciar e responder a incidentes de segurança (Barros, 2023).

No cenário educacional brasileiro, a diretriz Computação na Educação Básica: Documento Complementar à BNCC (Brasil, 2022), reforça a importância de desenvolver competências digitais desde o ensino fundamental. Especificamente para o 9º ano, no eixo Mundo Digital, o objeto de conhecimento Segurança Cibernética destaca, por meio da habilidade EF09CO04, a necessidade de os estudantes compreenderem o funcionamento de malwares e outros ataques cibernéticos, além de promoverem o uso ético e responsável das tecnologias, conforme o Quadro 1.

Quadro 1: Habilidade de Computação - Segurança Cibernética (BNCC – Complemento).

Objeto de conhecimento	Habilidade	Explicação da Habilidade
Segurança cibernética	(EF09CO04) Compreender o funcionamento de malwares e outros ataques cibernéticos.	Software malicioso, ou malware, são programas nocivos que obtêm acesso ilegal a dispositivos digitais. Eles podem acessar um computador ou dispositivo por meio de anexos de e-mail, pendrives ou sites desprotegidos. O malware pode invadir um computador e causar estragos. Esses programas podem desacelerar um dispositivo, enviar e-mails de spam ou até mesmo roubar ou excluir dados pessoais. O malware é classificado com base em como entrar no computador e no que faz quando está lá. Alguns exemplos de malware são: vírus, worms, rootkits, spyware, trojans, backdoors, ransomware, entre outros.

Adicionalmente, a Lei Geral de Proteção de Dados (LGPD) — Lei n.º 13.709/2018 (Brasil, 2018) estabelece instruções claras sobre o tratamento de dados pessoais, incluindo o uso de

informações de menores de idade em plataformas digitais. Essa legislação não apenas ressalta o papel fundamental da escola em promover práticas e orientações que respeitem a privacidade e a segurança digital, mas também amplia sua responsabilidade no processo de formação de cidadãos conscientes de seus direitos e deveres no ambiente online.

Nessa perspectiva, para compreender a amplitude dos desafios e das soluções em segurança digital, as próximas subseções detalham os principais riscos e ataques cibernéticos enfrentados atualmente e, em seguida, apresentam as técnicas de cibersegurança essenciais para mitigar essas ameaças.

2.1 Principais Riscos e Ataques Cibernéticos

O crescente uso de dispositivos digitais e a expansão das atividades online têm propiciado o surgimento de diversas ameaças cibernéticas que podem comprometer a segurança de usuários de todas as idades. No contexto escolar, e em particular com estudantes do 9º ano do ensino fundamental, a conscientização acerca desses riscos torna-se indispensável para fomentar práticas seguras e uma vivência mais responsável na internet (Brasil, 2022).

Conforme Hintzbergen et al. (2018), ataques cibernéticos podem ser compreendidos como quaisquer tentativas de danificar, modificar, desproteger, inutilizar, furtar ou explorar ativos digitais sem autorização, o que reforça a importância de medidas preventivas e de proteção contínua. Nesse sentido, as principais ameaças cibernéticas e suas respectivas definições, compreendidas a partir dos fascículos do CERT.br (2024) e dos estudos de Pande (2017), Stallings e Brown (2014) e Schappo (2022), são detalhadas no Quadro 2 a seguir.

Quadro 2: Principais ameaças cibernéticas.

Ameaças Cibernéticas	Definição
Vírus	Malware que se replica ao infectar arquivos ou programas, espalhando-se pelo sistema e causando danos.
Worm	Software malicioso que se replica e se espalha de forma autônoma por redes, sem necessitar de anexo a outros programas, podendo causar danos como consumo de largura de banda ou abertura de portas para ataques.
Trojan	Malware disfarçado de software legítimo, que enganam os usuários para que o instalem, permitindo que crackers (hackers mal-intencionados) acessem sistemas e roubem informações.
Ransomware	Programa de computador malicioso que criptografa arquivos e bloqueia o acesso ao sistema, exigindo um pagamento de resgate para a liberação dos dados.
Phishing	Técnica de engenharia social que enganam os usuários para que revelem informações sensíveis, como senhas e dados bancários, por meio de e-mails ou sites falsos.
Spyware	Programa de computador malicioso que monitora a atividade do usuário sem seu consentimento, coletando dados confidenciais, como senhas e histórico de navegação.
Negação de Serviço Distribuído (DDoS)	Ataque cibernético que sobrecarrega um sistema ou rede com um grande volume de tráfego, tornando-o inacessível para usuários legítimos.
Ataque de Força Bruta	Ocorre quando um cracker tenta adivinhar senhas por tentativa e erro, utilizando ferramentas automatizadas para testar diversas combinações até encontrar a correta.
Adware	Software que exibe propagandas indesejadas, muitas vezes rastreando a atividade do usuário para direcionar anúncios, podendo comprometer a privacidade e o desempenho do sistema.
Spam	Mensagens não solicitadas, geralmente de publicidade ou golpes, que podem sobrecarregar sistemas e dificultar o acesso a informações importantes.

A compreensão dessas ameaças cibernéticas, conforme detalhado no Quadro 2, é o ponto de partida para a construção de uma cultura de segurança digital mais precisa. Diante das crescentes tendências desses ataques e do desconhecimento dos danos causados por criminosos cibernéticos, conforme alertado por Schappo (2022), torna-se imperativo que a educação formal, especialmente no ensino fundamental, instrua os estudantes com o conhecimento necessário para identificar, prevenir e reagir a esses desafios, transformando-os em cidadãos digitais conscientes e proativos e minimizando os riscos com a utilização de ferramentas educacionais.

2.2 Técnicas de Cibersegurança

A implementação de técnicas de cibersegurança é fundamental para a proteção de ativos digitais e para o funcionamento confiável das organizações. Segundo Hintzbergen et al. (2018), a eficácia da segurança depende da adoção de um conjunto de medidas de controle, que abrangem políticas, processos, estruturas organizacionais, procedimentos e recursos tecnológicos. Esses controles devem ser continuamente monitorados, revisados e atualizados, a fim de garantir que os objetivos de segurança sejam alcançados.

Isso posto, as principais práticas de cibersegurança, fundamentadas nas obras de Pande (2017), Stallings e Brown (2014), Caruso (2013) e Faria (2014), são apresentadas no Quadro 3, evidenciando como a adoção dessas medidas surge como alicerce para a mitigação de potenciais riscos.

Quadro 3: Práticas de Cibersegurança.

Técnicas de cibersegurança	Definição
Cópias de segurança (backups)	Criação de duplicatas de dados e armazenamento em drives, dispositivos e em locais diferentes. Essa medida permite a recuperação dos dados em casos de falhas técnicas, erros operacionais, ataques cibernéticos ou desastres naturais.
Senhas fortes	Combinação de caracteres longa, complexa e única, que inclui letras maiúsculas e minúsculas, números e símbolos.
Autenticação multifatorial (MFA)	Método que exige que o usuário comprove sua identidade utilizando uma combinação de fatores de autenticação, como: algo que ele sabe (como uma senha), algo que ele possui (como um token físico ou digital) e/ou algo que ele é (como biometria).
Antivírus	Software desenvolvido para impedir a entrada de ameaças, identificar e eliminar códigos maliciosos. Todavia, é crucial que o usuário realize as atualizações recomendadas pelos fornecedores, visto que esses softwares recebem mecanismos para combater novos malwares e ataques cibernéticos.
Firewall	Implementados por meio de software, hardware ou uma combinação de ambos, atuam como barreiras entre redes internas e externas, controlando o tráfego de dados com base em regras de segurança. Quando corretamente configurados, contribuem para a prevenção de acessos não autorizados e ataques cibernéticos.
Redes privadas virtuais (VPN)	Permitem a criação de conexões seguras por meio de redes públicas, como a internet, utilizando protocolos de cifração e autenticação. São frequentemente utilizadas em ambientes corporativos para interligar redes locais (LANs) de diferentes unidades, garantindo a integridade e a confidencialidade dos dados transmitidos. Representam uma alternativa mais acessível às redes privadas com linhas dedicadas, mantendo altos níveis de segurança.

Embora essas técnicas sejam imprescindíveis, sua eficácia depende do monitoramento contínuo dos componentes digitais, o que permite identificar e corrigir falhas antes que comprometam os sistemas. Entre as medidas preventivas, destaca-se a atualização de softwares, frequentemente recomendada pelos próprios desenvolvedores para corrigir vulnerabilidades, melhorar o desempenho e fortalecer a proteção contra novas ameaças.

Hintzbergen et al. (2018) argumentam que a ausência dessas práticas representa uma vulnerabilidade explorável, elevando o risco de ataques e afetando negativamente a produtividade organizacional. Dessa forma, o constante monitoramento e atualização são práticas indispensáveis, juntamente com as técnicas de cibersegurança, para mitigar riscos e preservar a resiliência dos ativos digitais.

3 Metodologias Ativas

As metodologias ativas representam uma abordagem pedagógica centrada no estudante, na qual o processo de aprendizagem ocorre de forma participativa, crítica e reflexiva. Nessa perspectiva, o aluno é instigado a construir conhecimento por meio da investigação, da resolução de problemas e do descobrimento, em um ambiente educacional que envolve a atuação conjunta de professores, gestores, familiares e comunidade, compreendida como uma concepção de escola-comunidade de aprendizagem (Moran, 2019).

Essas metodologias, consoante com Marques et al. (2021), rompem com a lógica tradicional de ensino, na qual os estudantes são colocados em uma posição passiva, como meros receptores de informação. Ao contrário, as metodologias ativas promovem o protagonismo discente, favorecendo a autoaprendizagem, o desenvolvimento da criatividade e a interação entre pares e docentes, o que contribui para experiências de aprendizagem mais significativas.

Ademais, ainda que haja orientação e supervisão por parte do docente, a responsabilidade pela aprendizagem é compartilhada. Moran (2018) destaca que tanto no trabalho individual quanto nas atividades colaborativas, o avanço depende do envolvimento efetivo dos estudantes, da qualidade das interações, dos projetos desenvolvidos e da capacidade de sistematização dos conhecimentos adquiridos. Cabe ao professor atuar como mediador, orientador ou tutor, promovendo a autonomia e incentivando o envolvimento ativo dos alunos em todas as etapas do processo formativo.

Nesse sentido, as metodologias ativas abrangem diversas abordagens, entre as quais se incluem a sala de aula invertida, a programação, o ensino híbrido, a aprendizagem baseada em projetos, a ABJ e outras que podem estimular a autonomia e o protagonismo dos estudantes no processo de ensino e aprendizagem (Moran, 2018). Considerando essa diversidade de práticas pedagógicas ativas, nas subseções a seguir serão abordados alguns métodos relacionados a jogos (gamificação, jogos didáticos e ABJ), que apesar de apresentarem elementos comuns, possuem especificidades próprias.

3.1 Gamificação

Entre as práticas pedagógicas alinhadas às metodologias ativas, a gamificação destaca-se por sua ampla aplicação. De acordo com Silva Filho (2023), a gamificação pode ser adotada em diversas situações, sejam elas comerciais, recreativas e educativas, pois a gamificação geralmente envolve o uso de elementos comuns aos jogos — como metas, obstáculos, recompensas, feedback rápido e sistemas de pontuação. Esses elementos estimulam tanto a colaboração quanto a competição, características que fomentam a participação ativa dos participantes.

Conforme Eugenio (2020), essa abordagem se caracteriza pelo uso da lógica, da aparência e dos mecanismos de jogos na realidade, no intuito de influenciar a mudança de conduta. Assim, como argumenta Alves (2014), a gamificação não consiste em transformar atividades em jogos completos, mas sim em identificar e aplicar características lúdicas que podem enriquecer uma experiência, sem desconsiderar a realidade do contexto. Trata-se, portanto, de extrair dos jogos seus aspectos motivacionais e aplicá-los de forma intencional no ambiente educacional para atrair e engajar os estudantes.

A gamificação, segundo Silva Filho (2023), fundamenta-se em teorias psicológicas, especialmente na teoria da autodeterminação, a qual postula que a motivação humana depende da satisfação de três necessidades básicas: competência, autonomia e relacionamento. Sob essa ótica, o uso de elementos como pontuações, premiações, rankings, narrativas e o acompanhamento do progresso contribui para despertar e manter a motivação intrínseca dos estudantes, promovendo seu engajamento nas atividades de aprendizagem.

3.2 Jogos Didáticos

Enquanto a gamificação utiliza elementos de jogos em diversos contextos do processo pedagógico, os jogos didáticos correspondem ao uso de jogos elaborados e direcionados para o ensino de conteúdos específicos. Conforme Cunha (2012), esses jogos devem ser adotados como atividades intencionais voltadas ao ensino de conceitos e administradas pelo educador.

Antes de adentrar no conhecimento sobre jogos didáticos, é importante compreender o conceito de jogos, que de uma maneira geral, segundo Huizinga (2000), concerne a um fazer voluntário, delimitado por tempo e espaço específicos, regido por regras aceitas e obrigatórias, possui objetivo intrínseco e acompanhado por sensações de tensão, prazer e um distanciamento da realidade cotidiana.

O ato de jogar desencadeia uma série de fatores derivados da construção da narrativa, permeada por desafios, emoções e prazeres singulares. Seus fundamentos procedem de diversos

aspectos, tais como a possibilidade de comando, o feedback constante, a aprendizagem pela experiência, a interação cooperativa ou competitiva, além da versatilidade e da correta sequência das ações exigidas no ambiente lúdico (Carvalho, 2015).

Dessa forma, os jogos não devem ser percebidos apenas como entretenimento, haja vista que contribuem consideravelmente para o desenvolvimento social, emocional e cognitivo, permitindo ao indivíduo reconhecer limites, aplicar estratégias e otimizar sua formação (Fraga et al., 2023).

Sob a ótica de Leone et al. (2023), no âmbito educativo, a importância dos jogos é indubitável, podendo ser associados a diversos assuntos. No entanto, é indispensável o estudo, a pesquisa e o questionamento sobre os tipos de jogos disponíveis na literatura, sempre considerando a intencionalidade pedagógica e os propósitos do docente.

De acordo com Cunha (2012), vale ressaltar a distinção entre jogo educativo e jogo didático. Enquanto o primeiro abrange atividades ativas nas dimensões social, afetiva, cognitiva e física do estudante, orientadas pelo professor em diferentes ambientes, o segundo está diretamente vinculado ao ensino de conceitos e conteúdos.

Cunha (2012) explica que o jogo didático é estruturado por regras e atividades sistematizadas, mantendo um equilíbrio entre as funções lúdica e educativa, sendo mais comumente aplicado em sala de aula ou em laboratórios. Nesse contexto, Da Silva et al. (2025) destacam que os jogos aplicados em sala de aula podem ser tanto aqueles ajustados para fins educativos, quanto os elaborados e planejados especificamente para tal propósito, ou até mesmo os desenvolvidos pelos próprios estudantes em atividades de design de jogos.

3.3 Aprendizagem Baseada em Jogos

A Aprendizagem Baseada em Jogos (ABJ), para Carvalho (2015), representa uma abordagem pedagógica ampla que se manifesta na criação, utilização e aplicação de jogos no processo educacional e formativo. Essa metodologia integra o uso de elementos de gamificação e a aplicação de jogos didáticos e educativos em um conceito mais abrangente. A ABJ, assim, se alinha ao conceito mais amplo de Jogos Sérios (Serious Games), cujo objetivo primário não é o entretenimento, mas sim o alcance de metas específicas em áreas como educação, saúde, pesquisa e planejamento.

Complementando essa visão, Alves (2014) explica que a ABJ se materializa na criação de um sistema no qual os aprendizes se envolvem em um desafio com regras definidas, interagindo com o ambiente, recebendo e respondendo a feedbacks, com objetivos mensuráveis e despertando emoções ao longo da experiência.

A motivação, um ponto central destacado por Prensky (2012), é igualmente ressaltada por Moran (2018). Embora nenhum método de ensino seja universalmente eficaz, Prensky (2012) argumenta que a ABJ se sobressai por sua capacidade de motivar, oferecendo uma experiência educativa distinta das abordagens tradicionais. O autor atribui o sucesso dessa metodologia à combinação da motivação intrínseca ao jogo com a oferta de uma aprendizagem imediata e eficaz, que se distancia do modelo escolar convencional.

Essa atratividade é especialmente notória para as gerações que já têm o hábito de jogar, como aponta Moran (2018), pois a linguagem de desafios, recompensas, competição e cooperação é facilmente assimilada. Assim, jogos individuais ou coletivos, voltados à competição, colaboração ou estratégia, com fases bem estruturadas e habilidades claramente estabelecidas, têm se tornado cada vez mais comuns em diferentes áreas do conhecimento e em diversos níveis de ensino.

Adicionalmente, as capacidades desenvolvidas por meio dos jogos são notavelmente relevantes na ABJ. Fraga et al. (2023), por exemplo, descrevem os jogos de mesa como um campo de treinamento para a vida, destacando como eles estimulam a socialização, percepção cultural, autocontrole emocional e pensamento estratégico. Somando a essa perspectiva, Da Silva et al. (2025) sublinham que os jogos são uma ferramenta eficaz para trabalhar conceitos úteis à sociedade, como regularidade, limite, respeito e disciplina, uma vez que todas as ações no jogo são regidas por suas regras.

Mesmo para quem não tem experiência, o simples ato de jogar pode revelar e desenvolver habilidades antes desconhecidas, aplicáveis em diferentes contextos. Tais habilidades são potencializadas na gamificação no contexto da ABJ, que pode oferecer ambientes simulados e feedbacks instantâneos, consolidando essas competências de forma lúdica e imersiva. (Fraga et al., 2023).

Conforme os argumentos de Leone et al. (2023), para além de suas funções instrutivas, os jogos didáticos e educativos devem ser engajadores. Dessa forma, observa-se que as metodologias ativas, especialmente a gamificação, os jogos didáticos e a ABJ, oferecem estratégias inovadoras que potencializam a motivação e o engajamento dos estudantes, ao mesmo tempo em que promovem a construção de conhecimentos de maneira significativa.

4 Metodologia

Para este estudo, adotou-se uma abordagem quanti-qualitativa, visando compreender tanto os resultados objetivos quanto às percepções subjetivas dos participantes, o que promove uma análise integrada dos dados (Gil, 2017). A pesquisa possui natureza aplicada, com o objetivo de gerar conhecimentos práticos voltados à solução de problemas específicos e a interesses locais (Gerhardt; Silveira, 2009). Dessa forma, buscou-se avaliar a ABJ, a partir da aplicação do jogo Hacker-Ataque, no ensino e na conscientização sobre cibersegurança, analisando seu impacto e eficácia.

O estudo foi direcionado a duas turmas do 9º ano de uma escola municipal de ensino fundamental, em Castanhal (PA). A escolha da instituição baseou-se em sua disponibilidade, e a seleção dos estudantes do 9º ano justifica-se pela previsão de conteúdos de cibersegurança no documento de Computação complementar à BNCC (Brasil, 2022). O período de 07 a 23 de maio de 2025 foi dedicado aos diálogos e acordos com a escola, incluindo a definição da data de aplicação, elaboração de termos e divulgação. A aplicação do jogo Hacker-Ataque e a coleta de dados ocorreu no dia 23 de maio de 2025, das 14h às 17h, com autorização da coordenação escolar.

O estudo foi conduzido em seis etapas sequenciais: (1) revisão bibliográfica; (2) desenvolvimento do jogo Hacker-Ataque; (3) aplicação do questionário inicial; (4) implementação do jogo em sala de aula; (5) aplicação do questionário final; e (6) análise dos dados. A coleta de dados ocorreu em um único dia para minimizar interferências na rotina escolar.

Na revisão bibliográfica, buscou-se compreender como a ABJ vem sendo trabalhada na conscientização e ensino de cibersegurança no ambiente educacional, sobretudo no ensino fundamental II. Entre setembro de 2024 e março de 2025, foram utilizados os termos de busca: (“Cibersegurança” OR “Segurança da informação” OR “Segurança cibernética”) AND “Aprendizagem baseada em jogos” nas principais bases de dados científicos nacionais: RBIE (Revista Brasileira de Informática na Educação), RENOTE (Revista Novas Tecnologias na Educação), Portal de Periódicos da Capes, BD (Biblioteca Digital Brasileira de Teses e Dissertações), e os anais dos eventos do Congresso da Sociedade Brasileira de Computação

(WIE, WEI, SBIE, Workshops do CBIE e Workshop de Informática na Escola), indexados na base da Comissão Especial de Informática na Educação (CEIE), vinculada à SBC.

Como critérios de inclusão, foram considerados estudos que abordam a ABJ no ensino de cibersegurança, como artigos completos, teses, dissertações e trabalhos de conclusão de curso publicados entre os anos de 2021 e 2025. Foram excluídos os estudos voltados ao contexto corporativo, os trabalhos duplicados (mantendo-se a versão mais completa); as pesquisas cujo acesso não estava disponível de forma gratuita e aquelas que tratam a cibersegurança apenas de forma tangencial. Seguida essa etapa, realizou-se uma síntese comparativa dos estudos identificados.

A escolha do modelo analógico para o jogo se deve à sua acessibilidade, permitindo sua aplicação independentemente da disponibilidade de tecnologia digital. Esse formato proporciona uma experiência tangível e interativa, estimulando a colaboração e a socialização entre os estudantes.

Os dados foram coletados por meio de questionários e observação participante. Os questionários, aplicados antes e após a implementação do jogo, avaliaram o conhecimento prévio e as mudanças na compreensão dos estudantes. A pesquisa de observação participante, aquela em que o pesquisador, para observar os fenômenos, vivencia a experiência dos sujeitos estudados, participando de maneira sistemática e contínua em suas atividades ao longo do período da pesquisa (Severino, 2017), permitiu, durante a implementação do jogo, observar as interações dos estudantes, incluindo reações, nível de engajamento, compreensão da mecânica do jogo e a relevância do jogo para a assimilação de conceitos e conscientização sobre cibersegurança.

A análise dos dados compreendeu a estatística descritiva, utilizada para comparar os resultados dos questionários pré e pós-intervenção. Adicionalmente, empregou-se a análise de conteúdo, conforme Bardin (2016), para interpretar as observações e as percepções dos participantes, proporcionando uma avaliação abrangente dos impactos da metodologia adotada.

Apesar deste estudo não ter sido submetido a um comitê de ética em pesquisa, procurou-se assegurar que todos os cuidados éticos fossem tomados para a realização deste trabalho. A atividade foi de caráter pedagógico, sem riscos adicionais aos participantes, e contou com a anuência formal da coordenação da escola, por meio da assinatura de um Termo de Consentimento Livre e Esclarecido (TCLE), garantindo a anonimização dos dados e o uso seguro e restrito para fins acadêmicos.

Os recursos utilizados incluíram o Hacker-Ataque, jogo de tabuleiro desenvolvido especificamente para este estudo, questionários impressos, planilhas eletrônicas para tabulação e análise dos dados. Esses materiais asseguraram a implementação adequada da metodologia e a obtenção de resultados consistentes.

5 Trabalhos Relacionados

A ABJ se mostra uma estratégia pedagógica atraente e inovadora. Ela cria um processo de ensino e aprendizado mais ativo, interativo e estimulante, o que comprovadamente aumenta a motivação e facilita a assimilação do conteúdo (Savi; Ulbricht, 2008). Contudo, quando se trata da aplicação dessa abordagem no ensino de cibersegurança no contexto do ensino fundamental, observa-se uma vacuidade de pesquisas para fomentar uma discussão. Isso ressalta a importância de novas investigações para explorar o potencial dessa composição.

Não obstante a quantidade reduzida de estudos identificados (seis no total, nenhum deles voltado especificamente ao ensino fundamental II), a literatura evidencia a relevância da ABJ

para o ensino de cibersegurança. Ferreira et al. (2024), por exemplo, conduziram uma revisão sistemática sobre jogos sérios anti-phishing como ferramenta de ensino, buscando entender a percepção dos jogadores. É relevante notar que a maioria das referências dessa revisão consistiu em materiais estrangeiros, evidenciando a concentração da pesquisa global nessa área e a escassez de produção científica brasileira sobre o assunto. Eles concluíram que a adoção de jogos bem planejados pode, de fato, aprimorar a capacidade dos participantes de identificar e bloquear tentativas de fraude online.

Ferreira et al. (2024) destacam que, embora eficazes, os estudos analisados focam predominantemente em adultos com alguma familiaridade tecnológica (universitários ou profissionais). Essa abordagem gera uma lacuna na investigação da percepção de usuários sem conhecimento prévio em cibersegurança, sublinhando a importância de metodologias que unem teoria e prática em um ambiente controlado. Os achados desses autores, portanto, reforçam a necessidade de expandir o escopo das pesquisas e metodologias de ensino em cibersegurança para além de públicos especializados, alcançando usuários sem familiaridade prévia na área.

Similarmente, Schappo (2022), ao desenvolver o jogo de tabuleiro com versões analógica e digital, Th3_Off1c3⁴, demonstrou que práticas lúdicas focadas em SI podem facilitar o aprendizado de conceitos cruciais, como engenharia social, malware e boas práticas de proteção. O jogo simula ataques cibernéticos e foi projetado para estudantes universitários oferecendo uma experiência cooperativa e presencial.

A aplicação do jogo Th3_Off1c3 resultou em uma melhora de 10% na média de acertos em avaliações de conhecimento, indicando sua eficácia como ferramenta de apoio para consolidar conceitos de SI. Além de aproximar os jogadores de cenários simulados, a natureza tátil das peças e a interação presencial fortaleceram a colaboração entre os participantes, contribuindo para a consolidação do conhecimento de forma tangível (Schappo, 2022).

Outro trabalho que se destaca é o de Abreu et al. (2024), que desenvolveram e avaliaram o jogo educacional "Encrypta: A missão da liga dos robôs" para ensinar cibersegurança a adolescentes. No jogo, os jogadores controlam uma equipe de robôs heróis em minijogos temáticos que abordam temas cruciais como a criação de senhas fortes, a identificação de e-mails de phishing, a detecção de sites maliciosos e a importância de backups. Testes de usabilidade e aprendizado com o público-alvo validaram a eficácia da ferramenta, constatando que os jogadores a consideraram visualmente atraente, eficaz na transmissão dos alertas sobre perigos virtuais e, principalmente, capaz de ensinar os conceitos, como demonstrado pelos resultados positivos em um quiz. O estudo concluiu que o jogo atingiu seu objetivo educacional, com planos de expandir os tópicos de segurança e melhorar a experiência em dispositivos móveis.

No trabalho de Cardoso (2024), foi desenvolvido e avaliado o aplicativo gamificado SaPhish, uma solução educacional que prioriza a conscientização humana sobre soluções técnicas de IA para capacitar usuários contra-ataques de phishing. A proposta, centrada no usuário como última linha de defesa, consiste em um aplicativo móvel que simula ataques reais de engenharia social por meio de desafios interativos, incorporando elementos de gamificação como ranking e pontuação, além de permitir a criação de grupos para treinamentos corporativos. A pesquisa com 27 participantes de diversas áreas revelou que, embora 81,5% já tivessem conhecimento prévio sobre o tema, 77,8% ainda haviam sido alvos de phishing, destacando a necessidade da iniciativa. Os resultados atestaram a eficácia da ferramenta: 92,6% dos usuários julgaram o conteúdo de fácil compreensão e 89% relataram que o sistema de rankings aumentou seu engajamento.

⁴ Disponível em: <https://tabletopia.com/playground/th3-off1c3-bhp3jq/play-now>.

Além disso, o estudo de Dias et al. (2025) desenvolveu e testou quizzes gamificados como ferramenta educacional contra golpes digitais, utilizando a metodologia Design Science Research e baseando-se na análise de 144 boletins de ocorrência de estelionato eletrônico que identificaram cinco golpes predominantes. Testados com 40 participantes de diferentes faixas etárias, os resultados mostraram que 97,5% dos usuários relataram compreender os padrões dos golpes após a utilização, com melhor desempenho entre jovens (19-35 anos) e maior dificuldade entre idosos (60+), indicando a necessidade de ajustes específicos para esse público. Os quizzes demonstraram ser uma estratégia promissora para educação em cibersegurança, com o estudo continuando em desenvolvimento para refinar as perguntas e criar novos artefatos mais adequados ao público idoso.

Em seguida, o trabalho de Santos et al. (2025) apresenta o desenvolvimento e avaliação do Cyber Defender, um jogo educativo desenvolvido em PyGame para ensino de cibersegurança que aborda phishing, ransomware e ataques DDoS através de minigames integrados em um ambiente de escritório em visão top-down. Avaliado por 18 participantes utilizando quatro metodologias consolidadas (MEEGA+, IAQJEd, Pro-Avalia JS e PAJED), o jogo demonstrou usabilidade acessível, desafio adequado e eficácia na aprendizagem dos conceitos, embora tenha apresentado limitações na interação social por ser uma experiência individual mediada por NPCs. Os resultados indicam que a ferramenta é promissora para educação em segurança digital, combinando successfully elementos gamificados como sistema de vidas e moedas com conteúdo educativo contextualizado.

Nessa perspectiva, o presente estudo se diferencia ao desenvolver e aplicar o jogo de Hacker-Ataque para o ensino e conscientização de cibersegurança a estudantes do 9º ano do ensino fundamental, tendo como base o complemento à computação da BNCC (Brasil, 2022). Esse foco justifica-se pela incipiência de trabalhos para este público e pela presunção de ausência de conhecimento formal em cibersegurança no ambiente escolar. Outrossim, o modelo analógico apresenta-se como uma estratégia de inclusão a ambientes desprovidos de tecnologias digitais e pode proporcionar experiências táteis e mais colaborativas.

6 Concepção do Jogo Hacker-Ataque

Fundamentado nesses referenciais sobre cibersegurança e no potencial da ABJ, concebeu-se o Hacker-Ataque, um jogo de tabuleiro analógico com propósito didático. Seu desenvolvimento visou simular, de maneira prática e divertida, as principais ameaças cibernéticas e as estratégias defensivas correspondentes. Essa simulação se concretiza por meio de um sistema de trilhas interconectadas, cartas temáticas que representam tipos de ataques cibernéticos e técnicas de defesas, e desafios progressivos que estimulam o raciocínio estratégico dos jogadores.

O nome “Hacker-Ataque” foi escolhido por sua concisão e impacto, comunicando diretamente o cerne do jogo: a simulação de ameaças cibernéticas. “Hacker” evoca o contexto da segurança digital, enquanto “Ataque” explicita a dinâmica de confronto presente na mecânica do jogo. A combinação visa criar um título memorável e relevante, sinalizando a natureza educativa e estratégica da experiência ao familiarizar os jogadores com os desafios do cenário da cibersegurança.

6.1 Design e componentes do jogo Hacker-Ataque

Os componentes físicos do jogo, compreendendo o tabuleiro e as cartas, foram desenvolvidos utilizando a plataforma Canva⁵, uma plataforma online de design gráfico reconhecida por sua interface intuitiva e ampla variedade de recursos visuais. As imagens temáticas presentes nas

⁵ Disponível em: https://www.canva.com/pt_br/.

cartas foram criadas com o auxílio de Inteligência Artificial (IA), utilizando ferramentas como o ChatGPT⁶, Gemini⁷ e a funcionalidade de IA integrada ao próprio Canva. Complementarmente, o jogo inclui um dado e quatro marcadores (peões ou tokens), um para cada jogador, que são utilizados para a movimentação e interação no tabuleiro.

Conforme ilustrado na Figura 1, o tabuleiro do jogo Hacker-Ataque mede 42 x 58 centímetros e é estruturado em quatro trilhas, cada uma com uma cor distinta (laranja, roxa, rosa e verde). Partindo de uma “zona de risco” central, essas trilhas convergem em direção às bordas, onde se localizam os “pontos de segurança” (um para cada jogador). Cada trilha é composta por 25 casas, sequencialmente numeradas juntamente com 10 “nós”, representados pelos círculos azuis escuros (Figura 1). Dentre esses nós, 6 são de interferência, caracterizados por serem pontos onde as trilhas se cruzam, e 4 são de não interferência, quando não há cruzamento entre as linhas.

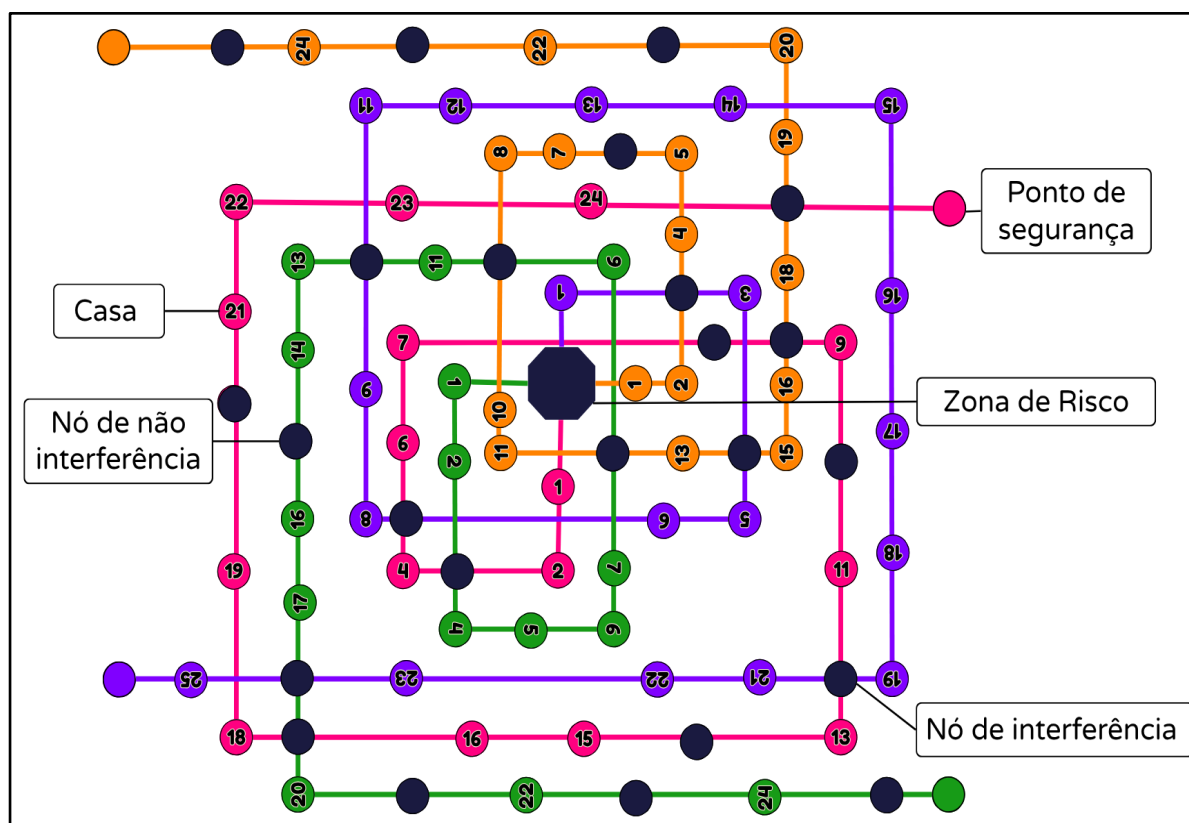


Figura 1: Tabuleiro do jogo Hacker-Ataque.

As cartas do jogo foram desenvolvidas seguindo um modelo visual padronizado, conforme ilustrado na Figura 2. Cada carta, seja de ataque ou de defesa, apresenta elementos-chave para a compreensão da mecânica e do conceito abordado, sendo distinguidas visualmente por suas cores: as cartas de ataque são vermelhas, enquanto as de defesa são verdes. No topo, encontra-se o nome do ataque (para cartas de ameaça, como “VÍRUS”) ou o nome da defesa (para cartas de proteção, como “ANTIVÍRUS”). O centro da carta é dedicado a uma ilustração representativa do tema. Na parte inferior, são detalhados o efeito da carta (indicando a consequência de um ataque) ou o bônus da carta (descrevendo o benefício de uma defesa). Além disso, cada carta de ataque inclui o conceito do ataque (uma breve definição da ameaça), e as cartas de defesa especificam a imunidade que conferem, listando os tipos de ameaças contra as quais são eficazes.

⁶ Disponível em: <https://chatgpt.com/>.

⁷ Disponível em: <https://gemini.google.com>.

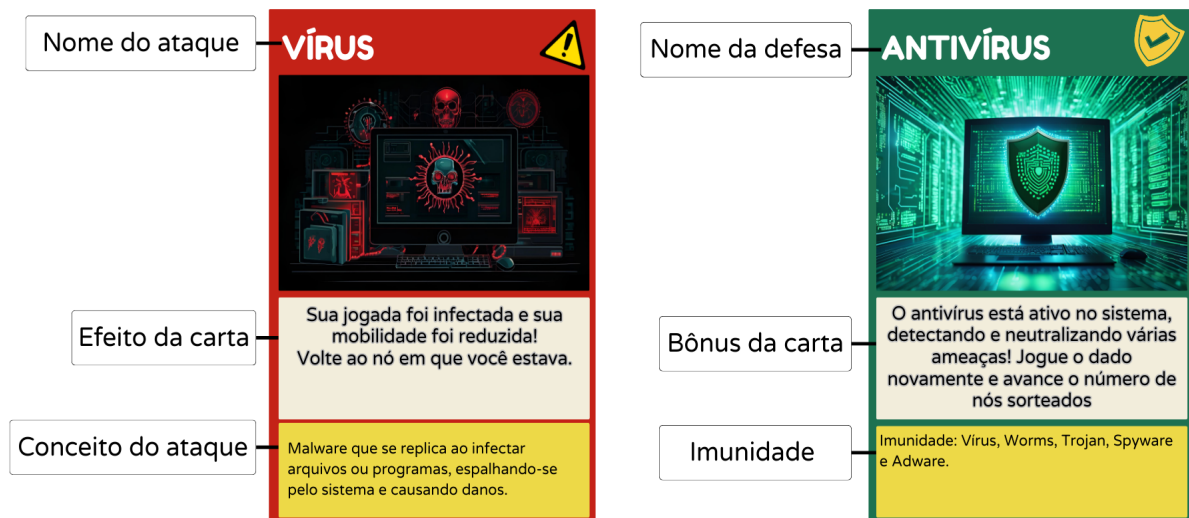


Figura 2: Identificação das cartas de defesa e ataque.

O Hacker-Ataque é composto por um total de 18 cartas, categorizadas em dois grupos principais. Dez dessas cartas representam tipos de malware e ataques cibernéticos mais recorrentes, incluindo: vírus, worms, trojan, ataque de força bruta, phishing, spyware, ransomware, adware, spam e DDoS (Figura 3). As oito cartas restantes correspondem às principais técnicas de cibersegurança: antivírus, firewall, VPN, senha forte, autenticação multifatorial, backup, atualização de software e monitoramento de sistema (Figura 4).



Figura 3: Todas as cartas de ataque.



Figura 4: Todas as cartas de defesa.

Em síntese, o *design* do jogo Hacker-Ataque, desde a concepção de seu tabuleiro interativo até a categorização e detalhamento das cartas, foi cuidadosamente planejado para criar uma experiência lúdica e instrutiva. A utilização de ferramentas de *design* e IA, aliada à clara distinção visual entre ataques e defesas, busca otimizar a imersão e facilitar a compreensão dos complexos conceitos de SI e cibersegurança.

6.2 Dinâmica e Mecânica do Jogo

Esse jogo pode ser jogado de 2 a 4 jogadores, os quais terão como desafio sair da “zona de risco” (no centro do tabuleiro) e alcançar o seu “ponto de segurança” (presente nas bordas do tabuleiro), conforme a Figura 1, superando ameaças cibernéticas e usando defesas estratégicas para evitar ataques ou conquistar bônus no decorrer das trilhas. O primeiro jogador a alcançar seu “ponto de segurança” é declarado vencedor, demonstrando conhecimento sobre os principais tipos de ataques e aplicando ações preventivas ao longo do caminho.

Cada partida dura em média de 15 a 20 minutos, antes de ser iniciada, as cartas são embaralhadas e cada jogador recebe quatro cartas aleatórias, e o avanço pela trilha se dá pelo arremesso de um dado, a partir do qual, o número sorteado corresponde ao número de casa que jogador deverá avançar, sendo usado tokens para marca a casa ou o nó em que o jogador está localizado.

No decorrer das trilhas, os jogadores podem parar em nós (Figura 1), onde o jogador compra uma carta e em seguida, deve escolher: usar os bônus de uma de suas cartas de defesa; ou usar uma de suas cartas de ataque contra um oponente. Nos nós de interferência, o jogador deve atacar o oponente que cruzar sua trilha, e nos nós sem interferência, o jogador escolhe de forma aleatória qual oponente atacar.

Entretanto, se o oponente tiver uma carta de defesa adequada, a ameaça é rebatida e o atacante sofre as consequências da própria carta sem direito a defesa. Se o oponente não tiver carta de defesa, ele deve cumprir as consequências da carta recebida. Contudo, se a carta de defesa for usada para defesa, ela não poderá mais ser usada como bônus.

7 Análise de Resultados

Os estudos de Ferreira et al. (2024), Schappo (2022), Abreu et al. (2024), Cardoso (2024), Dias et al. (2025) e Santos et al. (2025) evidenciam, em conjunto, o sólido potencial da ABJ e outras metodologias ativas para o ensino de cibersegurança. A revisão sistemática de Ferreira et al. (2024) estabelece um panorama geral, concluindo que jogos bem planejados são efetivos para melhorar a capacidade de identificar fraudes online. No entanto, este mesmo trabalho alerta para uma concentração da pesquisa em públicos com familiaridade tecnológica, como universitários e profissionais, gerando uma lacuna crucial na investigação sobre usuários sem conhecimentos prévios.

Essa limitação de público é um ponto comum na maioria dos trabalhos analisados. O jogo Th3_Off1c3 de Schappo (2022) foi desenvolvido para universitários, e o Encrypta de Abreu et al. (2024) focou em adolescentes, enquanto os artefatos de Cardoso (2024) e Santos et al. (2025) foram testados com públicos predominantemente jovens ou adultos. Nenhum deles foi direcionado ao ensino fundamental. O estudo de Dias et al. (2025) é que validar empiricamente essa lacuna, ao demonstrar que, embora os quizzes gamificados tenham sido eficazes, os idosos (acima de 60 anos) tiveram maior dificuldade, indicando a necessidade premente de adaptar as ferramentas para esse público.

Além do público-alvo, os estudos revelam uma diversidade de formatos e metodologias. Predominam as soluções digitais e de natureza individual, como o aplicativo SaPhish, os quizzes de Dias et al. e o jogo Cyber Defender — que, inclusive, apontou a limitação na interação social por ser uma experiência individual. Em contraste, o trabalho de Schappo (2022) se destaca ao propor um jogo de tabuleiro com versão digital, enfatizando a experiência presencial, cooperativa e tátil. Esse formato é uma alternativa valiosa para contextos desprovidos de recursos digitais robustos e ressalta a carência de mais pesquisas que explorem experiências colaborativas e não puramente digitais.

Quanto à eficácia, todos os artefatos desenvolvidos reportaram resultados positivos. Schappo (2022) registrou uma melhora mensurável de 10% nas avaliações de conhecimento, enquanto Abreu et al. (2024) e Santos et al. (2025) validaram a aprendizagem por meio de quizzes e metodologias consolidadas. Na esfera do engajamento e percepção, Cardoso (2024) constatou que quase 90% dos usuários se sentiram mais motivados pelo sistema de rankings, e Dias et al. (2025) obtiveram um índice de 97,5% de compreensão dos padrões de golpes entre os participantes.

Em síntese, a análise confirma que a ABJ é uma ferramenta versátil para a educação em cibersegurança, capaz de transmitir conceitos de forma engajadora. Contudo, os trabalhos coletivamente apontam para duas grandes lacunas futuras: a necessidade de expandir o escopo para públicos menos familiarizados com a tecnologia, como crianças do ensino fundamental e idosos, e a oportunidade de diversificar os formatos, investindo mais em experiências colaborativas e analógicas que complementam o predomínio atual das soluções digitais e individuais.

Nesse entendimento, a aplicação desta pesquisa foi realizada no contraturno das aulas de duas turmas do 9º ano do ensino fundamental. As inscrições foram divulgadas pela coordenação da escola, totalizando 20 estudantes inscritos. No dia 23 de maio de 2025, compareceram 12 participantes na escola, que faz parte da rede pública de ensino municipal de Castanhal (PA).

Com o objetivo de avaliar o conhecimento dos alunos e a eficácia do jogo de tabuleiro como ferramenta educacional, aplicou-se um questionário antes e após a implementação. O questionário aplicado antes do jogo foi composto por duas questões, abordando um total de 18 conceitos: a primeira, com dez conceitos (de A a J), tratou dos principais riscos e ataques

cibernéticos; a segunda, com oito conceitos (de A a H), abordou as principais técnicas de cibersegurança. O intuito foi compreender o nível de conhecimento prévio dos participantes.

O segundo questionário, aplicado após a realização do jogo, manteve as questões do questionário pré-jogo. Essa estratégia permitiu comparar as respostas dos participantes antes e depois da intervenção, possibilitando a análise do impacto do jogo de tabuleiro Hacker-Ataque no aprimoramento dos conhecimentos relacionados à segurança cibernética, bem como identificar possíveis avanços na compreensão dos conceitos abordados.

Para a Questão 1 do questionário pré-jogo (Quadro 4) sobre ameaças cibernéticas, os participantes demonstraram um conhecimento variado sobre os diferentes tipos de ataques. As ameaças Spam e Worm se destacaram com os maiores índices de acerto, seis e quatro respectivamente, seguidas de Força Bruta, também com quatro acertos. Por outro lado, o ataque de DDoS foi o único que nenhum participante conseguiu identificar corretamente, revelando uma clara lacuna de conhecimento sobre essa ameaça em específico.

Quadro 4: Respostas da Questão 1 pré-jogo.

Ameaça	Resposta mais associada	Acertos	Percentual de acertos	Respostas erradas
A.Worm	Worm (4) ✓	4	33.3%	Vírus, Ransomware, Força Bruta, Adware (2)
B.Trojan	Spam, Vírus (3)	1	8.3%	Spam, Vírus (3); Worm, Phishing (2); Adware (1)
C.Phishing	Ransomware (3)	1	8.3%	Ransomware (3); Worm, Trojan, DDoS, Spam, Adware, Vírus, Força Bruta, Spyware (1)
D.Ransomware	Phishing (4)	3	25.0%	Trojan (3), DDoS, Força Bruta (1)
E.DDoS	Vírus, Phishing (3)	0	0%	Vírus, Phishing (3); Trojan (2); Worm, Ransomware, Adware, Força Bruta (1)
F.Spam	Spam (6) ✓	6	50.0%	Trojan (2); Ransomware, Vírus, Força Bruta, Spyware (1)
G.Adware	Spyware (5)	2	16.7%	DDoS (2); Trojan, Phishing, Spam (1)
H.Vírus	Spyware, DDoS (4)	2	16.7%	Worm, Spam (1)
I.Força Bruta	Força Bruta (4) ✓	4	33.3%	DDoS (3); Adware (2); Trojan, Phishing, Ransomware (1)
J.Spyware	Worm, Adware (3)	1	8.3%	Worm, Adware (3); Força Bruta (2); Trojan, Ransomware, DDoS(1)

Os resultados também apontaram uma significativa confusão entre conceitos-chave de segurança. Houve uma notável troca entre Spyware e Adware, onde a resposta mais associada a um foi justamente o outro. De modo similar, Phishing e Ransomware foram frequentemente confundidos entre si, assim como Trojan e Vírus tiveram baixos índices de acerto. Esses equívocos indicam que, embora alguns termos sejam familiares, suas definições e características distintivas não estão totalmente claras para a maioria dos participantes.

O Quadro 5 apresenta os resultados da Questão 1 do questionário pós-jogo, aplicado após a atividade de aprendizagem, mostrando a evolução no reconhecimento das ameaças cibernéticas. De forma geral, observa-se uma melhoria significativa no número de acertos em comparação com o teste pré-jogo. Ameaças como Força Bruta e Trojan tiveram bons desempenhos, com dez e nove acertos respectivamente, enquanto Spam, Spyware, Ransomware e Phishing também apresentaram altos índices de acerto, variando entre seis e nove. O DDoS também apresentou um número moderado de acertos (cinco), mas ainda foi confundido com Phishing e Ransomware por alguns participantes.

Quadro 5: Respostas da Questão 1 pós-jogo.

Ameaça	Resposta mais associada	Acertos	percentual de acertos	Respostas erradas
A.Worm	Vírus (8)	3	25.0%	Vírus (8); Força Bruta (1)
B.Trojan	Trojan (9) ✓	9	75.0%	DDoS (2); Ransomware (1)
C.Phishing	Phishing (6) ✓	6	50.0%	Worm (4), Adware (2)
D.Ransomware	Ransomware (7) ✓	7	58.3%	Adware (2); Worm, Phishing, Força Bruta (1)
E.DDoS	DDoS (5) ✓	5	41.7%	Phishing, Ransomware (3); Spam (1)
F.Spam	Spam (8) ✓	8	66.7%	Phishing, Ransomware, Adware, Spyware (1)
G.Adware	Adware (6) ✓	6	50.0%	Trojan, DDoS (2); Spam, Vírus (1)
H.Vírus	Worm (4)	1	8.3%	Worm (4); DDoS, Adware (2); Spam (1)
I.Força Bruta	Força Bruta (10) ✓	10	83.3%	Phishing, Ransomware (1)
J.Spyware	Spyware (9) ✓	9	75.0%	DDoS, Spam, Adware (1)

Nos conceitos A e H da primeira questão, que tratam de worms e vírus, respectivamente, observou-se que a maioria dos participantes confundiram os conceitos, ambos classificados como malwares e descritos de forma semelhante nas cartas do jogo, como é possível observar nas Figuras 5 e 6. Essa semelhança contribuiu para um aumento significativo no percentual de erros no segundo questionário, indicando que, apesar da intervenção, ainda houve dificuldade na distinção entre esses dois tipos de ameaças cibernéticas. Esse resultado sugere a necessidade de reforçar a diferenciação conceitual entre vírus e worms em futuras aplicações do jogo.

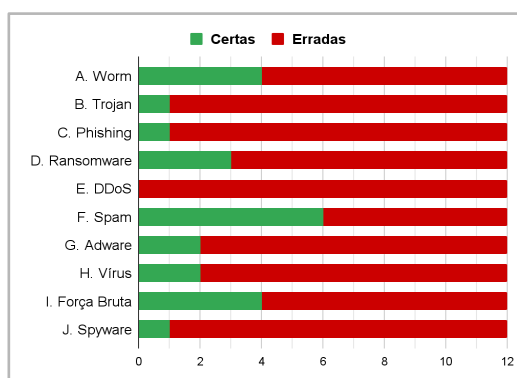


Figura 5: Resultados gerais da Questão 1 do questionário pré-jogo.

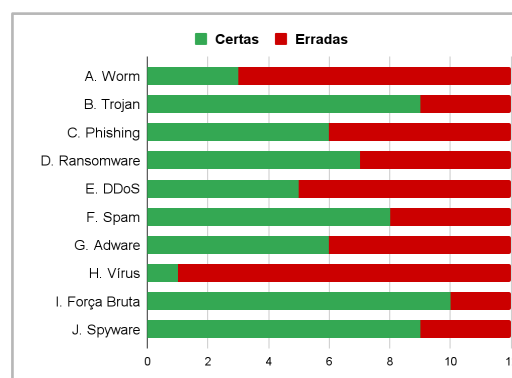


Figura 6: Resultados gerais da Questão 1 do questionário pós-jogo.

A quantidade de acertos obtidos após a realização do jogo revelou-se relevante, demonstrando que os participantes conseguiram assimilar de forma mais eficaz os conceitos relacionados aos principais ataques cibernéticos. Esse resultado evidencia o potencial do jogo de tabuleiro Hacker-Ataque como uma ferramenta didática capaz de facilitar a aprendizagem e a assimilação de conteúdos complexos, promovendo um melhor entendimento das ameaças no contexto da SI.

Houve uma melhoria significativa no desempenho dos participantes após a atividade de aprendizado. O número de acertos mais do que dobrou, passando de 24 para 64. Em termos percentuais, a participação dos acertos do pós-jogo corresponde a quase três quartos do total de respostas corretas consideradas, enquanto o pré-jogo representa pouco mais de um quarto (Figura 7).

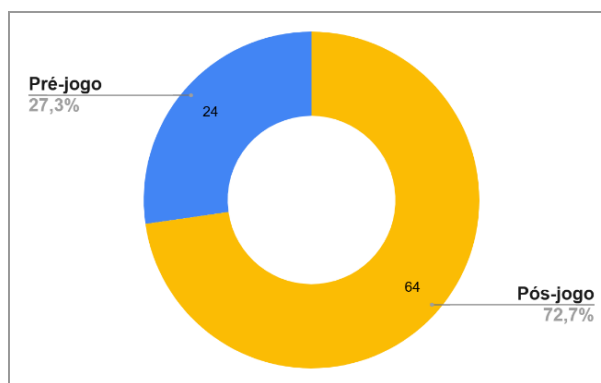


Figura 7: Gráfico com o percentual de acertos da Questão 1.

De maneira geral, os participantes demonstraram um bom conhecimento inicial sobre os conceitos básicos de segurança. As técnicas de Backup e Senha Forte obtiveram o melhor desempenho, com dez acertos cada, indicando que são conceitos bem consolidados. Firewall e Monitoramento de Sistema também tiveram um alto índice de reconhecimento, com sete e oito acertos, respectivamente (Quadro 6).

Quadro 6: Respostas da Questão 2 pré-jogo.

Técnicas de defesa	Resposta mais associada	Acertos	Percentual de acertos	Respostas erradas
A.Firewall	Firewall (7) ✓	7	58.3%	Antivírus (5)
B.Autenticação Multifatorial	Autentificação Multifatorial (5) ✓	5	41.7%	Firewall (4); Antivírus (2); VPN(1)
C.Antivírus	Antivírus (5) ✓	5	41.7%	VPN (3); Firewall, Senha forte, Atualização de Software, Monitoramento de sistema (1)
D.Backup	Backup (10) ✓	10	83.3%	Atualização de Software, Monitoramento de sistema (1)
E.VPN	VPN (5) ✓	5	41.7%	Autenticação Multifatorial (4); Backup, Senha forte, Atualização de Software (1)
F.Senha forte	Senha forte (10) ✓	10	83.3%	Autenticação Multifatorial, Backup (1)
G.Atualização de Software	Atualização de Software (6) ✓	6	50.0%	Autenticação Multifatorial, VPN, Atualização de Software (2)
H.Monitoramento de sistema	Monitoramento de sistema (8) ✓	8	66.7%	Atualização de Software (3); VPN (1)

No entanto, algumas confusões conceituais foram evidentes. A principal delas foi entre Firewall e Antivírus, onde cinco participantes associaram a primeira à segunda. A Autenticação Multifatorial também foi comumente confundida com Firewall e, em menor escala, com VPN e Antivírus. A técnica VPN foi erroneamente ligada à Autenticação Multifatorial por quatro participantes. Esses equívocos revelam uma certa sobreposição ou falta de clareza na compreensão das funções específicas de cada medida de segurança.

O Quadro 7 apresenta os resultados da Questão 2 no pós-jogo, mostrando a evolução do conhecimento dos participantes sobre técnicas de defesa cibernética após a atividade educativa. De forma geral, houve uma melhoria significativa e consolidação do aprendizado, com a maioria das técnicas sendo corretamente identificadas pela maioria dos participantes.

Quadro 7: Respostas da Questão 2 pós-jogo.

Técnicas de defesa	Resposta mais associada	Acertos	Percentual de acertos	Respostas erradas
A.Firewall	Firewall (9) ✓	9	75.0%	Senha forte (2); VPN (1)
B.Autenticação Multifatorial	Autenticação Multifatorial (5) ✓	5	41.7%	Antivírus, VPN, Monitoramento de sistema (2); Firewall (1)
C.Antivírus	Antivírus (6) ✓	6	50.0%	Autenticação Multifatorial (3); Backup (2); Senha forte (1)
D.Backup	Backup (9) ✓	9	75.0%	Antivírus, Firewall, Senha forte (1)
E.VPN	VPN (5) ✓	5	41.7%	Antivírus, Autenticação Multifatorial (2); Backup, Senha forte, Atualização de Software (1)
F.Senha forte	Senha forte (7) ✓	7	58.3%	Atualização de Software (3); Monitoramento de sistema (2)
G.Atualização de Software	Atualização de Software (7) ✓	7	58.3%	VPN (2); Antivírus, Firewall, Autenticação Multifatorial (1)
H.Monitoramento de sistema	Monitoramento de sistema (8) ✓	8	66.7%	Atualização de Software, VPN (2)

Os maiores índices de acerto foram alcançados por Firewall (nove), Backup (nove), Monitoramento de Sistema (nove), Senha Forte (sete) e Atualização de Software (sete), indicando que os conceitos dessas defesas foram bem compreendidos. Técnicas como Antivírus (seis), VPN (cinco) e Autenticação Multifatorial (cinco), embora com um número menor de acertos absolutos, mantiveram ou melhoraram sua taxa de reconhecimento.

As confusões que persistiram foram mais específicas. A Autenticação Multifatorial continuou a ser um ponto de dificuldade, sendo confundida com Antivírus, VPN e Monitoramento. A VPN também foi ocasionalmente associada a outras técnicas, como Antivírus e Autenticação Multifatorial. Esses dados mostram que, enquanto os conceitos fundamentais foram solidificados, as funções específicas de algumas ferramentas digitais ainda podem gerar dúvidas.

Portanto, em relação aos conceitos das principais técnicas de defesa, abordados na Questão 2, observou-se uma quantidade expressiva de acertos, o que evidencia a presença de um aprendizado prévio adquirido em situações anteriores. Esse resultado, ilustrado na Figura 8, sugere que alguns participantes já possuíam algum conhecimento sobre essas técnicas antes da aplicação do jogo, o que pode ter contribuído para um desempenho mais consistente nessa parte da avaliação.

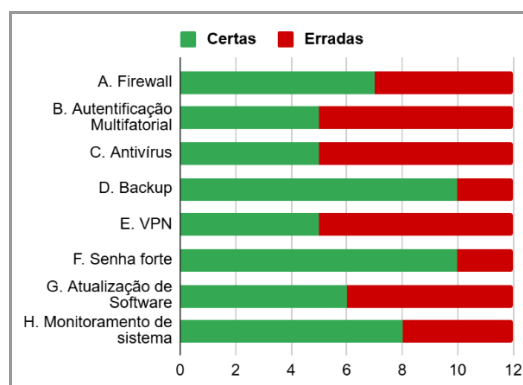


Figura 8: Resultados gerais da Questão 2 do questionário pré-jogo.

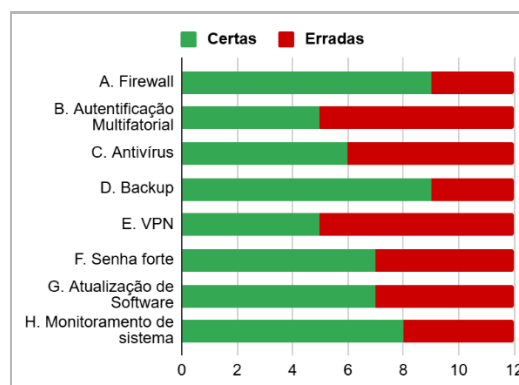


Figura 9: Resultados gerais da Questão 2 do questionário pós-jogo.

Na Questão 2 do questionário pós-jogo (Figura 9), não foi observada uma mudança expressiva em comparação com os resultados do questionário pré-jogo. No entanto, alguns aspectos específicos merecem destaque: houve um aumento no número de acertos relacionados aos conceitos de firewall, antivírus e atualização de software, indicando uma melhor compreensão dessas práticas de defesa após a intervenção. Por outro lado, verificou-se um aumento nos erros associados aos conceitos de backup e senha forte. Os demais conceitos mantiveram um quantitativo estável de acertos e erros, demonstrando consistência no desempenho dos participantes em relação a esses conteúdos.

Este resultado indica que, ao contrário da Questão 1, houve poucas mudanças no desempenho geral dos participantes na identificação das técnicas de defesa após a atividade de aprendizado. O conhecimento prévio do grupo sobre o assunto já era bom e se manteve estável. O jogo ou intervenção educativa, portanto, não produziu um ganho mensurável de aprendizado nesse tópico específico.

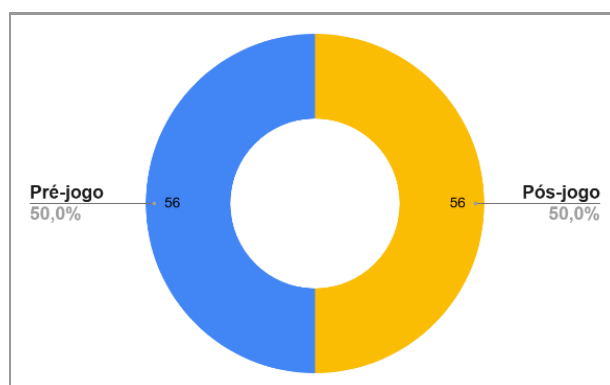


Figura 10: Gráfico com o percentual de acertos da Questão 2.

Dessa forma, é possível observar um aumento significativo no percentual acumulado de acertos, que passou de 80 para 120, representando uma elevação de 40% para 60% na taxa de acertos do questionário pré-jogo para o pós-jogo, respectivamente (Figura 9).

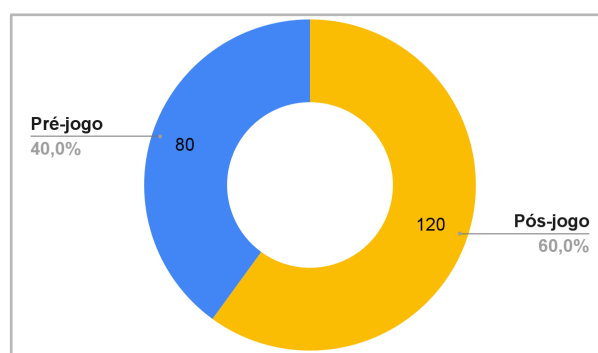


Figura 11: Gráfico com o percentual acumulado de acertos dos questionários.

Esses resultados evidenciam a efetividade do jogo de tabuleiro Hacker-Ataque como ferramenta pedagógica, ao proporcionar uma melhora considerável no desempenho dos participantes e favorecer a assimilação dos conceitos relacionados à segurança cibernética.

7.1 Avaliação da Experiência dos Jogadores

No segundo questionário, além da avaliação dos conhecimentos dos participantes, foram incluídas questões específicas para investigar a experiência com o jogo. Essa avaliação foi composta por três perguntas em escala de 1 a 5, visando mensurar aspectos como engajamento,

entendimento das regras do jogo e interação entre os participantes, além de uma questão aberta, destinada a coletar outras percepções qualitativas sobre a atividade. Essa combinação permitiu obter uma visão mais ampla e detalhada sobre a eficácia do jogo não apenas como ferramenta didática, mas também como recurso lúdico e motivacional.

Na Questão 3, buscou-se avaliar o nível de engajamento dos participantes em relação à sua participação no jogo (Figura 12). A pergunta visava compreender o quanto a atividade conseguiu despertar interesse e manter a atenção dos jogadores ao longo da partida, aspectos fundamentais para a efetividade de abordagens lúdicas no processo de ensino-aprendizagem.

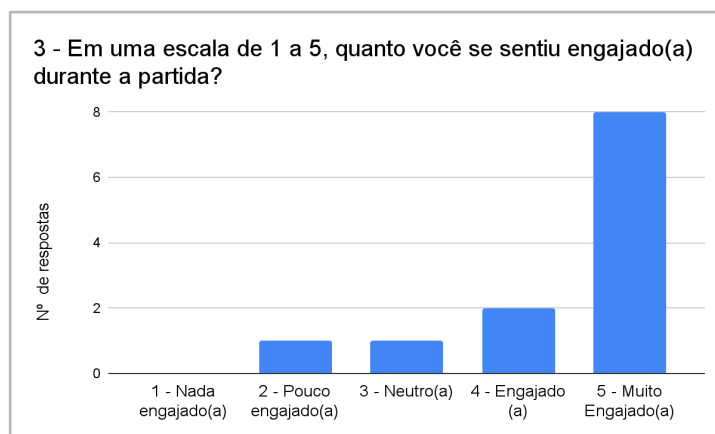


Figura 12: Gráfico com o nível de engajamento.

Na Questão 4, o objetivo foi avaliar se as regras do jogo foram apresentadas de maneira clara e se os participantes as consideraram fáceis de entender e aprender (Figura 13). Essa avaliação é fundamental para verificar a acessibilidade do jogo, bem como sua adequação como ferramenta pedagógica, já que regras complexas ou mal elaboradas podem comprometer a dinâmica, reduzir o engajamento e prejudicar a assimilação dos conteúdos propostos.

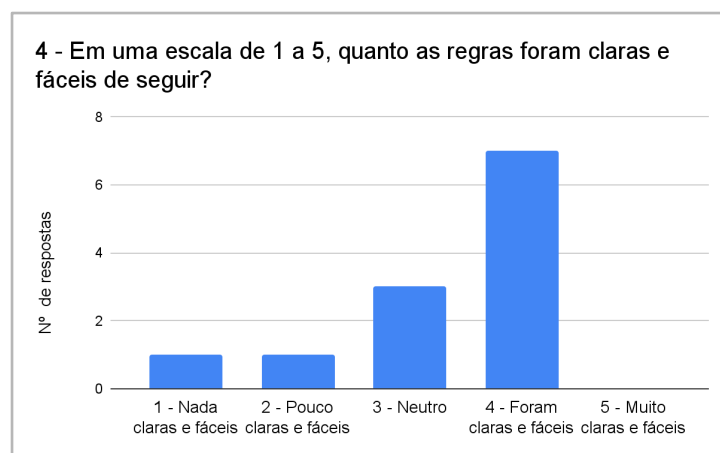


Figura 13: Gráfico com o nível de clareza e facilidade das regras.

Na Questão 5, o objetivo foi avaliar a qualidade da interação dos participantes com o jogo de tabuleiro (Figura 14). Essa análise buscou compreender como os jogadores se relacionaram com a dinâmica proposta, incluindo aspectos como colaboração, competitividade e troca de informações.

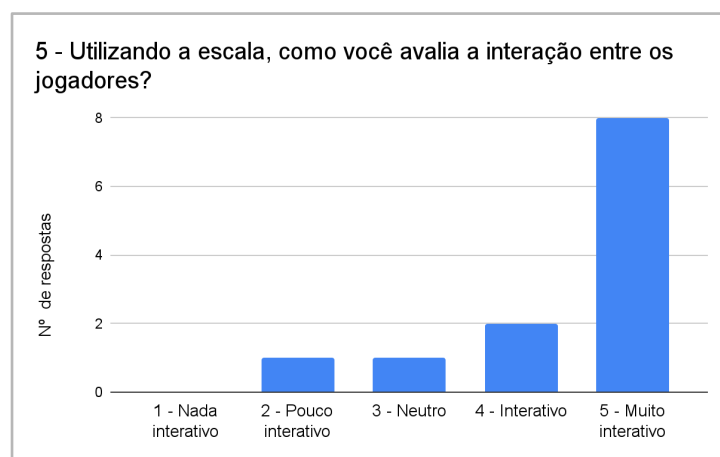


Figura 14: Gráfico com o nível de interação.

Na Questão 6, os participantes foram convidados a descrever livremente suas experiências com o jogo, proporcionando comentários sobre a atividade (Quadro 8). As respostas indicaram, em sua maioria, percepções positivas, destacando aspectos como diversão, interatividade, aprendizagem e desejo de repetir a experiência. Termos como “muito boa”, “engraçada”, “empolgante” e “educativo” foram frequentemente utilizados, evidenciando que o jogo conseguiu não apenas transmitir conteúdos relacionados à segurança cibernética, mas também criar um ambiente lúdico e agradável.

Quadro 8: Experiência com o jogo.

6 - Como você descreveria sua experiência geral com o jogo?	
“Foi uma experiência muito boa e engraçada.”	“Foi mais ou menos, não joguei direito.”
“Mais ou menos.”	“Ótimas, até porque eu gostei.”
“Muito boa, foi engraçada e empolgante.”	“Foi divertido e educativo.”
“Gostei bastante e adoraria jogar mais vezes.”	“Bom achei muito legal uma experiência única aprendi bastante.”
“Muito boa, foi engraçado e empolgante.”	“Muito boa e divertida, um jogo bastante interativo, muito bom.”

Embora algumas respostas tenham indicado uma experiência mais neutra ou limitada, como “mais ou menos” ou “não joguei direito”, essas observações podem sinalizar oportunidades de melhoria na condução da atividade, como ajustes na explicação das regras ou na dinâmica do jogo. No geral, os relatos reforçam o potencial do jogo de tabuleiro Hacker-Ataque como uma ferramenta eficaz para promover o engajamento, a aprendizagem e a socialização entre os participantes.

8 Considerações Finais

A partir dos resultados apresentados, a análise da eficácia da ABJ, por meio do jogo Hacker-Ataque, demonstrou ser uma metodologia assertiva e auspiciosa para o ensino e conscientização sobre cibersegurança para alunos do 9º ano do ensino fundamental. Os dados quantitativos de aumento de acertos, aliados à percepção qualitativa de engajamento e diversão por parte dos participantes, evidenciam que a ABJ não só é capaz de transmitir conhecimentos complexos de forma eficiente, mas também de cultivar o interesse e a conscientização sobre um tema de vital importância no mundo digital atual. As pequenas dificuldades pontuais, como a diferenciação

entre vírus e worms, são aprendizados para refinamentos futuros, mas não ofuscam o sucesso geral da intervenção e do alcance dos objetivos desta pesquisa.

A relevância deste estudo no cenário educacional e social contemporâneo é indubitável. Ao abordar a cibersegurança, um tema de urgência global diante da crescente exposição de crianças e adolescentes a riscos online, a pesquisa oferece uma contribuição direta para a formação de cidadãos digitalmente conscientes e seguros. Sua importância reside não apenas na identificação de uma necessidade crítica, mas principalmente na proposição e validação de metodologias ativas, em especial a ABJ, no ensino e conscientização da cibersegurança. Este trabalho, portanto, não só se alinha às demandas do documento de Computação complemento à BNCC de 2022 por competências digitais, mas também pavimenta o caminho para que educadores e escolas desenvolvam abordagens mais dinâmicas e eficazes no preparo das novas gerações para os desafios do mundo digital.

É pertinente destacar que o êxito desta pesquisa, desenvolvida por concluintes do curso de Licenciatura em Informática, ressalta a importância da atuação do licenciado em informática na educação básica. Tal profissional é fundamental para o cumprimento das competências e habilidades propostas pelo complemento da BNCC (Brasil, 2022) referente à Computação. Isso se deve ao fato de que, além de possuir conhecimentos técnicos relacionados à computação, ele também é capacitado a conceber, desenvolver e integrar práticas pedagógicas que atendam às demandas do processo de ensino-aprendizagem no âmbito das tecnologias digitais de informação e comunicação.

Considerando os achados e as limitações do estudo, como o número de participantes e o foco em uma única escola, que podem não permitir a generalização completa dos resultados para todas as realidades escolares, sugere-se, como ações futuras, a expansão da pesquisa não apenas para o 9º ano, mas também para um público mais amplo, incluindo outras faixas etárias e contextos educacionais, a fim de validar e aprimorar a metodologia da ABJ no ensino de cibersegurança. Além disso, recomenda-se um estudo aprofundado sobre o refinamento do jogo Hacker-Ataque, bem como a elaboração de sua versão digital, visando a ampliação de seu alcance e aplicabilidade.

Em suma, a presente pesquisa não apenas valida a ABJ como uma metodologia didática eficaz para o ensino de cibersegurança no ensino fundamental, mas também sublinha a necessidade imperativa de valorizar e integrar o professor licenciado em informática na educação básica brasileira. Ao capacitar os estudantes com o conhecimento e as habilidades necessárias para navegar no mundo digital de forma segura e ética, a educação se estabelece como um alicerce fundamental para a construção de uma cidadania digital responsável e consciente. Dessa forma, investir em abordagens inovadoras e no profissional que as pode aplicar efetivamente é crucial para proteger as futuras gerações dos riscos cibernéticos e empondera-las para o uso construtivo e transformador das tecnologias digitais.

Referências

- Abreu, J., Miani, R., & Nomura, S. (2024). "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*, (pp. 1327-1338). Porto Alegre: SBC. <https://doi:10.5753/sbgames.2024.240133>. [GS Search].
- Alves, F. G. (2014). *Como criar experiências de aprendizagem engajadoras: um guia completo do conceito à prática*. DVS editora, 2º edição. [GS Search].

- Associação Brasileira de Normas Técnicas (ABNT). (2013). *NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos*. Rio de Janeiro: ABNT.
- Bardin, L. (2016). *Análise de Conteúdo*/Laurence Bardin; tradução Luís Antero Reto, Augusto Pinheiro.- São Paulo: Edições 70, 2016. [GS Search].
- Barros, J. A. A. D. (2023). *Segurança cibernética nas escolas e universidades brasileiras: avaliando a inserção da educação cibernética no sistema educacional brasileiro e seus efeitos na prevenção de incidentes cibernéticos*. <https://repositorio.esg.br/handle/123456789/1756>. [GS Search].
- Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018: Dispõe sobre a proteção de dados pessoais*. Diário Oficial da União. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. [GS Search].
- Brasil, Ministério da Educação. (2022). *Computação: Complemento à BNCC – Base Nacional Comum Curricular*. https://basenacionalcomum.mec.gov.br/images/historico/anexo_parecer_cneceb_n_2_2022_bncc_computacao.pdf. [GS Search].
- Cardoso, V. W. (2024). *Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo Phishing*. Trabalho de Conclusão de Curso, Universidade Federal do Rio de Janeiro. <https://pantheon.ufrj.br/bitstream/11422/23611/1/VWCardoso.pdf>. [GS Search].
- Caruso, C. A. A., & Steffen, F. D. (2013). *Segurança em informática e de informações* (4ª ed.). São Paulo: SENAC.
- Carvalho, C. V. de (2015). Aprendizagem baseada em jogos-Game-based learning. In *II World Congress on Systems Engineering and Information Technology* (pp. 176-181). [GS Search].
- CERT.br. (2024). *Cartilhas de segurança para internet: Fascículos*. CERT.br. <https://cartilha.cert.br/fasciculos/#furto-de-celular>.
- Comitê Gestor da Internet no Brasil (CGI.br). (2023). *TIC Kids Online Brasil: Microdados TIC Kids Online Brasil 2024 – Pais e responsáveis*. <https://cetic.br/pt/pesquisa/kids-online/analises/>. [GS Search].
- Check Point Research. (2024). *Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years – A 30% Increase in Q2 2024 Global Cyber Attacks*. Check Point Blog. <https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/>.
- Cunha, M. B. da (2012). Jogos no ensino de química: considerações teóricas para sua utilização em sala de aula. *Química Nova na Escola*, São Paulo,[s. L.], 34(2), 92-98. [GS Search].
- Da Silva, C. A. F., de Souza Matos, E., Zabet, D., Dias, G. O. M., & dos Santos, J. M. O. (2025). "O Jogo é a Prova!": um relato sobre o uso de jogo educacional articulado ao raciocínio computacional nos Anos Finais do Ensino Fundamental. *Revista Brasileira de Informática na Educação*, 33, 130-151. <https://doi.org/10.5753/rbie.2025.3323>. [GS Search].
- Dias, A., Santos, L., Valério, R., Souza, P., Araujo, N., & Silva, A. (2025). O Uso de Quizzes como Ferramenta para Educação em Cibersegurança. In *Anais da I Escola Regional de Sistemas de Informação de Mato Grosso*, (pp. 91-101). Porto Alegre: SBC. <https://doi:10.5753/ersimt.2025.8868>. [GS Search].
- Eugenio, T. (2020). *Aula em jogo: descomplicando a gamificação para educadores*. Évora. [GS Search].

- Faria, H. M. de. (2014). *Bacula: Ferramenta livre de backup* (2ª ed.). Rio de Janeiro: Brasport. [GS Search].
- Ferreira, A. L. H., de Sales, A. B., Ferreira, A. E., & Palmeira, E. G. (2024). Características dos jogos sérios Anti-Phishing como ferramenta de ensino: uma revisão sistemática. *Revista Novas Tecnologias na Educação*, 22(1), 340-350. DOI: <https://doi.org/10.22456/1679-1916.141560>. [GS Search].
- Fraga, E. A. G., & Moraes, R. D. P. G. (2023). Jogos Tradicionais e seus Impactos no Desenvolvimento de Habilidades. *Serious Games: do Lúdico à Educação*. Ponta Grossa, PR: Atena, 37. [GS Search].
- Gerhardt, T. E., & Silveira, D. T. (2009). *Métodos de pesquisa* (1ª ed.). Editora da UFRGS. [GS Search].
- Gil, A. C. (2017). *Como Elaborar projeto de Pesquisa*. (6ª ed.) São Paulo: Atlas.
- Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. Brasport.
- Huizinga, J. (2000). *Homo ludens: O jogo como elemento da cultura*. São Paulo: Perspectiva.
- Kaspersky. (2023). *Brasil é o país com mais ataques a dispositivos móveis na América Latina*. <https://www.kaspersky.com.br/blog/brasil-recebe-mais-ataques-america-latina/21782>.
- Leone, F. R., Pinto, C. G. C., Rocha, F. R., & Barros, M. C. (2023). Evolução dos jogos na educação. In R. Bernhard et al. (Orgs.), *Serious Games: do Lúdico à Educação* (pp. 1-19). Atena. [GS Search].
- Marques, H. R., Campos, A. C., Andrade, D. M., & Zambalde, A. L. (2021). Inovação no ensino: uma revisão sistemática das metodologias ativas de ensino-aprendizagem. *Avaliação: Revista da Avaliação da Educação Superior (Campinas)*, 26(03), 718-741. <https://periodicos.uniso.br/avaliacao/article/view/4815>. [GS Search].
- Moran, J. (2018). Metodologias ativas para uma aprendizagem mais profunda. In *Metodologias ativas para uma educação inovadora: uma abordagem teórico-prática*. Porto Alegre: Penso, 35-76. [GS Search].
- Moran, J. (2019). *Metodologias ativas de bolso: como os alunos podem aprender de forma ativa, simplificada e profunda*. Arco 43. [GS Search].
- Núcleo de Informação e Coordenação do Ponto BR – NIC.br. (2025). *TIC Educação 2024: Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras* [livro eletrônico]. Comitê Gestor da Internet no Brasil (CGI.br). https://cetic.br/media/docs/publicacoes/2/pt/20251027173400/tic_educacao_2024_livro_eletronico.pdf.
- Pande, J. (2017). *Introdução à segurança cibernética*. Haldwani: Uttarakhand Open University. [GS Search].
- Prensky, M. (2012). *Aprendizagem baseada em jogos digitais*. Editora Senac São Paulo. [GS Search].
- Santos, E., Campano Junior, M., Silva, F., & Aylon, L. (2025). Cyber Defender: desenvolvimento e avaliação de um jogo educativo para ensino de segurança cibernética. In *Anais do XXV Simpósio Brasileiro de Cibersegurança*, (pp. 289-304). Porto Alegre: SBC. <https://doi.org/10.5753/sbseg.2025.10588>. [GS Search].

- Savi, R., & Ulbricht, V. R. (2008). Jogos digitais educacionais: benefícios e desafios. *Revista Novas Tecnologias na Educação*, 6(1). DOI: <https://doi.org/10.22456/1679-1916.14405>. [GS Search].
- Schappo, F. M. (2022). *TH3_OFFIC3: um jogo de tabuleiro educacional para o ensino de conceitos da segurança da informação*. <https://repositorio.ufsm.br/handle/1/27304>.
- Severino, A. J. (2017). *Metodologia do trabalho científico*. Cortez editora. [GS Search].
- Silva Filho, F. B. D. (2023). *A gamificação e o professor reflexivo de robótica educacional: um estudo de caso*. [GS Search].
- Stallings, W., & Brown, L. B. (2014). *Segurança de computadores: princípios e práticas* (A. S. Marques, Trad.; 2ª ed.). Elsevier. [GS Search].

Apêndices

QUESTIONÁRIO PRÉ-JOGO

1- Relacionar cada tipo de malware ou ataque cibernético com sua definição correta.

Instruções:

1. Leia as definições na coluna **B**.
2. Associe cada termo da coluna **A** à sua descrição correspondente.

Coluna A (Termos)	Coluna B (Definições)
1. Vírus ()	A. Malware que se replica rapidamente por redes, consumindo recursos sem infectar arquivos específicos.
2. Worm ()	B. Software malicioso disfarçado de programa legítimo, permitindo acesso não autorizado.
3. Trojan ()	C. Técnica que engana usuários para obter informações confidenciais por meio de e-mails ou sites falsos.
4. Ransomware ()	D. Malware que criptografa arquivos e exige pagamento para liberá-los.
5. Phishing ()	E. Ataque que sobrecarrega um sistema com tráfego, tornando-o inacessível.
6. Spyware ()	F. Mensagens indesejadas (geralmente golpes ou propagandas) que sobrecarregam sistemas.
7. DDoS ()	G. Software que exibe anúncios invasivos e rastreia a atividade do usuário.
8. Força Bruta ()	H. Malware que se espalha infectando arquivos ou programas.
9. Spam ()	I. Técnica de tentativa e erro para descobrir senhas.
10. Adware ()	J. Malware que monitora atividades do usuário sem consentimento.

Respostas Corretas: 1. *H* | 2. *A* | 3. *B* | 4. *D* | 5. *C* | 6. *J* | 7. *E* | 8. *I* | 9. *F* | 10. *G*

2 - Associar cada termo de segurança digital à sua definição correta.

Instruções:

1. Leia as definições na Coluna **B**.
2. Relacione cada termo da Coluna **A** à descrição correspondente.

Coluna A (Termos)	Coluna B (Definições)
1. Antivírus ()	A. Sistema que controla o tráfego de rede, bloqueando acessos não autorizados.
2. Firewall ()	B. Método de segurança que exige múltiplas formas de verificação de identidade (ex.: senha + código SMS).
3. Backup ()	C. Ferramenta que detecta, bloqueia e remove malwares de um dispositivo.
4. Senha Forte ()	D. Cópia de segurança de dados importantes para recuperação em caso de perda.
5. Autenticação Multifatorial ()	E. Rede privada que criptografa a conexão, protegendo dados em redes públicas.
6. Atualização de Software ()	F. Senha complexa, com combinação de letras, números e símbolos, difícil de ser descoberta.

7. VPN ()	G. Correções lançadas por desenvolvedores para corrigir falhas de segurança em programas.
8. Monitoramento de Sistema ()	H. Processo de observar atividades em um computador ou rede para detectar ameaças ou falhas.

Respostas Corretas: 1. C | 2. A | 3. D | 4. F | 5. B | 6. G | 7. E | 8. H

QUESTIONÁRIO PÓS-JOGO

1- Relacionar cada tipo de malware ou ataque cibernético com sua definição correta.

Instruções:

3. Leia as definições na coluna B.

4. Associe cada termo da coluna A à sua descrição correspondente.

Coluna A (Termos)	Coluna B (Definições)
1. Vírus ()	A. Malware que se replica rapidamente por redes, consumindo recursos sem infectar arquivos específicos.
2. Worm ()	B. Software malicioso disfarçado de programa legítimo, permitindo acesso não autorizado.
3. Trojan ()	C. Técnica que engana usuários para obter informações confidenciais por meio de e-mails ou sites falsos.
4. Ransomware ()	D. Malware que criptografa arquivos e exige pagamento para liberá-los.
5. Phishing ()	E. Ataque que sobrecarrega um sistema com tráfego, tornando-o inacessível.
6. Spyware ()	F. Mensagens indesejadas (geralmente golpes ou propagandas) que sobrecarregam sistemas.
7. DDoS ()	G. Software que exibe anúncios invasivos e rastreia a atividade do usuário.
8. Força Bruta ()	H. Malware que se espalha infectando arquivos ou programas.
9. Spam ()	I. Técnica de tentativa e erro para descobrir senhas.
10. Adware ()	J. Malware que monitora atividades do usuário sem consentimento.

Respostas Corretas: 1. H | 2. A | 3. B | 4. D | 5. C | 6. J | 7. E | 8. I | 9. F | 10. G

2 - Associar cada termo de segurança digital à sua definição correta.

Instruções:

3. Leia as definições na Coluna B.

4. Relacione cada termo da Coluna A à descrição correspondente.

Coluna A (Termos)	Coluna B (Definições)
1. Antivírus ()	A. Sistema que controla o tráfego de rede, bloqueando acessos não autorizados.
2. Firewall ()	B. Método de segurança que exige múltiplas formas de verificação de identidade (ex.: senha + código SMS).
3. Backup ()	C. Ferramenta que detecta, bloqueia e remove malwares de um dispositivo.

4. Senha Forte ()	D. Cópia de segurança de dados importantes para recuperação em caso de perda.
5. Autenticação Multifatorial ()	E. Rede privada que criptografa a conexão, protegendo dados em redes públicas.
6. Atualização de Software ()	F. Senha complexa, com combinação de letras, números e símbolos, difícil de ser descoberta.
7. VPN ()	G. Correções lançadas por desenvolvedores para corrigir falhas de segurança em programas.
8. Monitoramento de Sistema ()	H. Processo de observar atividades em um computador ou rede para detectar ameaças ou falhas.

Respostas Corretas:

1. C | 2. A | 3. D | 4. F | 5. B | 6. G | 7. E | 8. H

3 - Em uma escala de 1 a 5, quanto você se sentiu engajado(a) durante a partida?

- () 1 - Nada engajado(a)
 () 2 - Pouco engajado(a)
 () 3 - Neutro(a)
 () 4 - Engajado(a)
 () 5 - Muito Engajado(a)

4 - Em uma escala de 1 a 5, quanto as regras foram claras e fáceis de seguir?

- () 1 - Nada claras e fáceis
 () 2 - Pouco claras e fáceis
 () 3 - Neutro
 () 4 - Foram claras e fáceis
 () 5 - Muito claras e fáceis

5 - Utilizando a escala, como você avalia a interação entre os jogadores?

1	2	3	4	5
				
Nada interativo	Pouco interativo	Neutro	Interativo	Muito interativo

6 - Como você descreveria sua experiência geral com o jogo?



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ

CAMPUS CASTANHAL

DIRETORIA DE PÓS-GRADUAÇÃO, PESQUISA E INOVAÇÃO

CURSO DE LICENCIATURA EM INFORMÁTICA



TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está recebendo este Termo de Consentimento Livre e Esclarecido (TCLE) para que autorize a participação de estudantes da turmas do 9º ano do turno da manhã da Escola Municipal de Ensino Fundamental (EMEF) Maria Inês Costa, para a realização da atividade intitulada **“APRENDIZAGEM BASEADA EM JOGOS: UMA ABORDAGEM PARA O ENSINO DE CIBERSEGURANÇA NO 9º ANO”**, a qual será ministrada em uma sala de aula, da referida escola, no dia 23 de maio de 2025 (sexta-feira), das 14h00 às 17h00. Este documento consiste em esclarecer os objetivos e os procedimentos da atividade para esta coordenação, de modo a atender às normas federais sobre ética na pesquisa.

Essa atividade forma parte da pesquisa em andamento desenvolvida pelos discentes Daniela Barbosa de Sousa, matrícula nº 20210933787, e Renan Anezio da Rocha, matrícula nº 20200931668 sob orientação do Prof. Esp. Franciel da Silva Amorim e da Me. Andréa Guimarães Ribeiro Ohashi, do curso de graduação Licenciatura em Informática, do IFPA – campus Castanhal, sobre o uso de jogos na educação, em especial, para aprimorar as habilidades de cibersegurança. O objetivo da atividade lúdica e interativa é que os alunos consigam identificar e compreender o funcionamento de malwares, ataques cibernéticos (EF09CO04) e técnicas de segurança, desenvolvendo a competência de Segurança Cibernética. Neste TCLE, constam os endereços de e-mail dos pesquisadores principais e dos professores orientadores, pelos quais poderão ser dirimidas quaisquer dúvidas sobre a aplicação da atividade ou outros assuntos referentes à própria pesquisa.

Durante a realização da proposta será aplicado um questionário pré-jogo e outro pós-jogo, para se identificar quais os conhecimentos dos estudantes sobre cibersegurança e quais as percepções sobre o uso de jogos no aprendizado, respectivamente. Durante a atividade, será feito o registro fotográfico, no entanto, considerando o fato de o público-alvo ser composto por adolescentes e jovens entre 14 e 18 anos e observados os princípios sobre o direito à imagem, serão salvaguardados os dados pessoais dos estudantes, os quais aparecerão na pesquisa sob o uso de pseudônimos.

A participação do(a) estudante é de forma voluntária, podendo esse(a) sair de sala caso não queira participar.

Eu, Auricélia de Jesus Alves de Oliveira, Coordenadora da EMEF Maria Inês Costa, declaro que li e compreendi o conteúdo deste TCLE e estou de acordo com os objetivos da atividade e de seus benefícios para a formação dos estudantes, pelos quais ora me responsabilizo, para

Página 1 de 2



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PARÁ
DIRETORIA DE PÓS-GRADUAÇÃO, PESQUISA E INOVAÇÃO
CURSO DE LICENCIATURA EM INFORMÁTICA

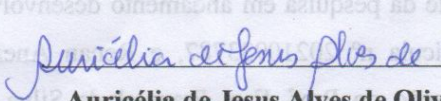


aquisição de conhecimento, e concordo com a participação deles nos termos deste documento.

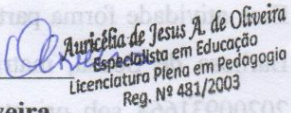
Por fim, autorizo, sem quaisquer restrições quanto aos efeitos patrimoniais e financeiros sobre de uso das informações obtidas a partir da participação na atividade, para serem utilizadas integralmente ou em partes, desde que seja para fins acadêmicos e/ou de pesquisa e/ou nas publicações provenientes da pesquisa, sem limitação de prazo e de citações, com a ressalva da proteção dos dados pessoais dos estudantes participantes, a partir da presente data.

Por ser expressão da verdade, firmo o presente termo, do qual estou recebendo uma cópia, para fins de direito.

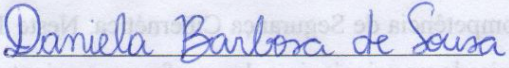
Castanhal, 23 de maio de 2025.



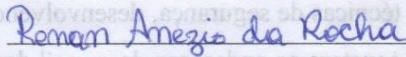
Auricélia de Jesus Alves de Oliveira
Coordenadora da Escola Municipal de Ensino Fundamental Maria Inês Costa
teiaalves74@gmail.com



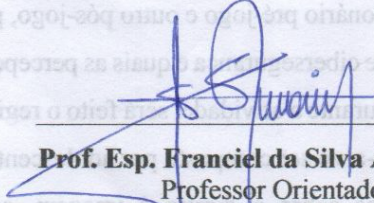
Auricélia de Jesus A. de Oliveira
Especialista em Educação
Licenciatura Plena em Pedagogia
Reg. Nº 481/2003



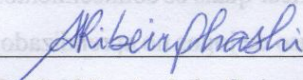
Daniela Barbosa de Sousa
Discente Pesquisadora
db085721@gmail.com



Renan Anezio da Rocha
Discente Pesquisador
renan18anezio@gmail.com



Prof. Esp. Franciel da Silva Amorim
Professor Orientador
franciel.amorim@ifpa.edu.br



Profa. Ma. Andréa Guimarães R. Ohashi
Professora Orientadora
andrea.ohashi@ifpa.edu.br

Página 2 de 2