JOGOS E CIBERSEGURANÇA: Relato de Experiência da aplicação do jogo híbrido Chapada Investigação no ensino médio

SILVA, Vinícius dos Reis [1]
SILVA, Victor Santos [2]
SOUZA, José Gustavo da Silva [3]
ANDRADE, Alêssa Soares de Oliveira [4]
ARAÚJO, Luís Gustavo de Jesus [5]

RESUMO: Este relato de experiência apresenta a implementação de uma aula plugada no ensino médio, utilizando um jogo de investigação como estratégia didática para explorar os conceitos de redes de computadores, como phishing, DNS, sniffer, segurança de dados e outros conceitos, em aula de desenvolvimento web. A proposta pedagógica visou promover a compreensão prática dos riscos associados a ataques digitais, através de uma atividade ativa e colaborativa. Durante a aula, os alunos foram organizados em equipes e desafiados a analisar situações simuladas, identificar tentativas de phishing e avaliar as evidências fornecidas para identificar o autor do crime. Os resultados observados demonstram que a utilização de metodologias ativas contribuiu de forma significativa para o engajamento dos estudantes, favorecendo a participação, o pensamento crítico e a construção coletiva do conhecimento. Conclui-se que a aplicação de jogos investigativos em aulas plugadas é uma abordagem eficaz para o ensino de temas relacionados à cibersegurança, tornando o processo de ensino-aprendizagem mais dinâmico, significativo e alinhado às demandas contemporâneas da educação.

PALAVRAS-CHAVE: Cibersegurança; Phishing; Jogo de Investigação; Aula Plugada; Ensino Médio; Metodologias Ativas.

1 INTRODUÇÃO

A crescente presença das tecnologias digitais no dia a dia tem aumentado a necessidade de discutir questões relacionadas à cibersegurança nas escolas, especialmente no ensino médio, fase em que os alunos intensificam sua interação com a internet e plataformas digitais. Nesse cenário, é essencial abordar conceitos como phishing para formar usuários mais críticos e conscientes no ambiente virtual.

[1] Graduando em Licenciatura em Computação, Bolsista PIBID, Instituto Federal de Educação, Ciência e Tecnologia, *Campus* Jacobina, vinicciusre@email.com
[2] Graduando em Licenciatura em Computação, Bolsista PIBID, Instituto Federal de Educação, Ciência e Tecnologia, Campus Jacobina, victor.s.ifba@gmail.com
[3] Graduando em Licenciatura em Computação, Bolsista do Programa de Iniciação à Docência (PIBID), Instituto Federal de Educação, Ciência e Tecnologia da Bahia Campus Jacobina, tec.farmaciajosegustavo@gmail.com
[4] Mestre em Ciência da Computação, Bolsista e Supervisora do Programa Institucional de Iniciação à Docência (PIBID), Instituto Federal de Educação, Ciência e Tecnologia da Bahia, *Campus* Jacobina, alessaoliveira@ifba.edu.br
[5] Mestre em Computação aplicada, Bolsista e Supervisor do Programa Institucional de Iniciação à Docência (PIBID), Orientador desta pesquisa, Instituto Federal de Educação, Ciência e Tecnologia da Bahia, *Campus* Jacobina, luis_araujo@ifba.edu.br

Contudo, a complexidade desses temas requer a utilização de estratégias pedagógicas que tornem o processo de ensino-aprendizagem mais acessível, dinâmico e significativo.

A crescente presença das tecnologias na vida cotidiana dos estudantes torna essencial discutir questões de cibersegurança desde a educação básica. Com o uso constante da internet e de plataformas digitais, os riscos, como fraudes e vazamentos de dados, também se ampliam. Assim, é vital que a escola contribua para o desenvolvimento de uma postura crítica e consciente, algo que é reforçado pela BNCC Computação ao destacar competências relacionadas à segurança e à privacidade da informação, como trazido pela habilidade EF09CO04: "Compreender o funcionamento de malwares e outros ataques cibernéticos" (Brasil, 2022, p. 52).

Entre essas ameaças, o phishing se destaca por explorar o comportamento do usuário, exigindo não apenas conhecimento técnico, mas também atenção e senso crítico. Abordar esse tema em sala de aula ajuda os alunos a reconhecerem situações suspeitas e a tomarem decisões mais seguras no ambiente digital. Para isso, a aplicação de metodologias ativas faz uma grande diferença. Quando os alunos se envolvem de maneira mais direta, investigando, discutindo e resolvendo problemas, o aprendizado se torna mais significativo. Nesse contexto, os jogos investigativos aparecem como uma alternativa interessante, pois promovem o raciocínio, a colaboração e a análise de evidências, tornando o conteúdo mais próximo da realidade dos estudantes e mais fácil de compreender.

Estudos como o de Hassunuma et al. (2024) evidenciam o potencial destes tipos de jogos na educação, empregando estruturas fundamentadas em evidências e pistas para motivar os alunos. Particularmente na área de cibersegurança, Farias et al. (2019) e Schappo e Medina (2024) introduzem, respectivamente, o jogo Self Protect e o Th3Off1c3, que tratam de ameaças digitais como phishing, ransomware[6] e spyware[7], ressaltando a eficácia de métodos lúdicos para a compreensão desses conceitos.

Este trabalho é um relato de experiência desenvolvido no âmbito do Programa Institucional de Bolsa de Iniciação à Docência (PIBID), com a

[6] Tipo de malware que sequestra dados ou bloqueia sistemas, criptografando arquivos e exigindo resgate, como pagamentos, para liberá-los.
[7] Software malicioso (malware) que infecta eletrônicos para espionar atividades, coletar dados pessoais, como senhas e informações bancárias sem consentimento.

participação de nós, bolsistas Vinícius dos Reis Silva e Victor Santos Silva, sob a supervisão do professor Luís Gustavo de Jesus Araújo. A atividade foi planejada, desenvolvida e aplicada pelos próprios bolsistas e pelo supervisor em uma turma do ensino médio no Instituto Federal de Ciência e Tecnologia do Estado da Bahia, campus Jacobina, com o intuito de explorar o conceito de phishing no contexto da aula de desenvolvimento web através de uma abordagem diferenciada.

Para isso, foi criada uma aula no contexto da computação plugada baseada em um jogo de investigação, denominado “Chapada Investigação: Caso Cripto”, separado em duas partes, onde os alunos, organizados em equipes, foram desafiados a analisar situações simuladas, identificar a tentativa de *phishing* e interpretar evidências para resolver um caso proposto. A proposta buscou integrar metodologias ativas ao ensino de conteúdos técnicos, promovendo a participação dos alunos, o trabalho colaborativo e o desenvolvimento do pensamento crítico. Assim, a presente experiência tem como objetivo refletir sobre as contribuições do uso de atividades investigativas e colaborativas no ensino de cibersegurança, ressaltando o potencial dessas estratégias para promover uma aprendizagem mais significativa e alinhada às demandas contemporâneas da educação.

Figura 01. Capa do envelope digital 1 entregue aos alunos

Fonte: Elaborado pelos pesquisadores.

2 METODOLOGIA

A atividade foi realizada com base na metodologia IBP3A, abrangendo as fases de idealização, planejamento, preparação, aplicação e análise. Primeiramente, foi estabelecida a proposta de um jogo investigativo focado no ensino de conceitos de cibersegurança, especialmente o phishing, com o intuito de conectar o conteúdo à realidade dos alunos. Na fase de preparação, foram criados os materiais do jogo, que incluíam e-mails simulados, registros de rede, listas de personagens e pistas organizadas em etapas. Além disso, foram desenvolvidos perfis e elementos visuais para tornar a atividade mais envolvente.

A aplicação foi realizada em uma turma do Ensino Médio técnico em informática, com os alunos divididos em grupos. A dinâmica foi organizada em etapas progressivas, onde os estudantes analisavam pistas, identificavam tentativas de phishing e avançavam à medida que validavam suas respostas com os mediadores. Durante toda a atividade, houve monitoramento dos grupos, com orientações e validações previamente planejadas, assegurando a condução do jogo e o cumprimento dos objetivos estabelecidos.

3 RESULTADOS E DISCUSSÃO

Durante a execução, monitoramos de perto o progresso da atividade, atuando como mediadores entre as equipes e o desenvolvimento do caso. Um delegado foi implementado através de um chatbot por meio de um perfil do Whatsapp, o que facilitou a dinâmica da investigação e permitiu que os alunos validassem respostas e recebessem orientações ao longo do processo. A atividade foi realizada durante duas horas, e, nesse intervalo, fomos orientando a turma conforme cada grupo progredia nas etapas do jogo.

Na primeira etapa, os alunos tinham que identificar a técnica empregada no ataque, na segunda, deveriam descobrir quem estava por trás da ação e, na fase final, o desafio consistia em encontrar a senha utilizada para proteger os dados criptografados. Foi exatamente essa última fase que apresentou a maior dificuldade, pois demandou mais atenção, raciocínio e uma abordagem um pouco mais criativa para perceber a pista correta e relacionar os elementos disponíveis. Vale ressaltar que cada etapa possuiu instruções específicas e os alunos podiam recorrer ao delegado (*chatbot*) sempre que necessitasse.

De maneira geral, os alunos se comportaram de forma engajada e mostraram interesse pela proposta, mas alguns grupos necessitaram de mais suporte para conseguir avançar, especialmente nas fases em que era preciso interpretar melhor as pistas e relacionar as evidências apresentadas. Isso evidenciou que a atividade demandou acompanhamento constante tanto de nós, bolsistas, quanto do supervisor, o que foi crucial para manter o ritmo do jogo e ajudar os estudantes sem fornecer diretamente as respostas.

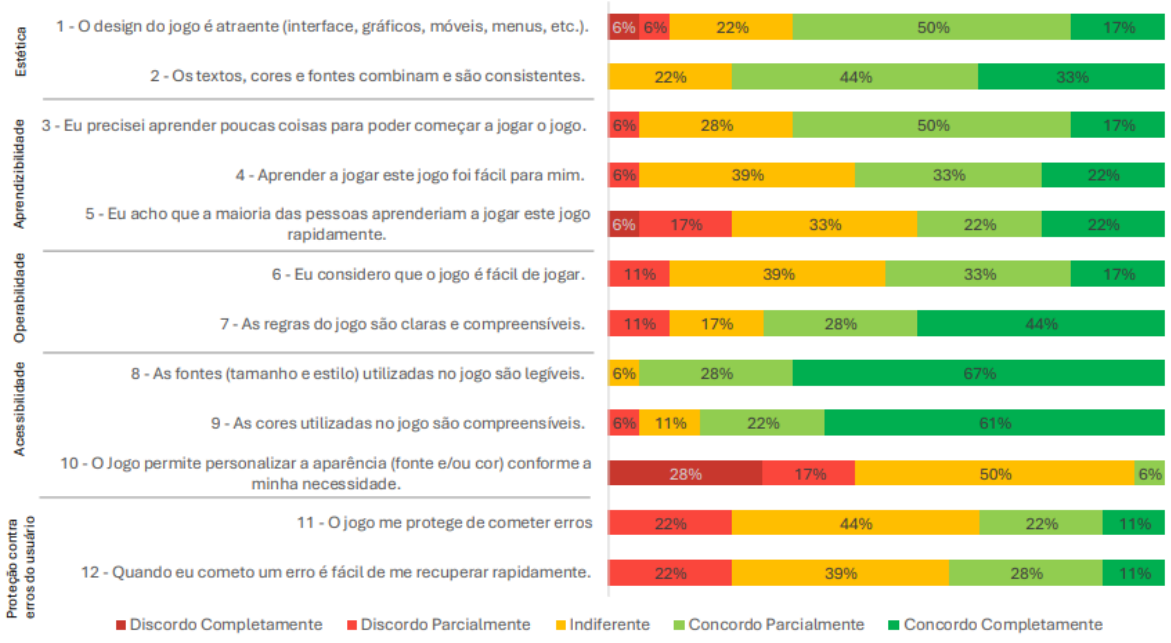
De maneira geral, a execução da atividade foi bastante positiva. A turma mostrou interesse ao longo de todo o processo, e o formato investigativo foi eficaz em manter os alunos engajados até o final. O trabalho em equipe também se destacou, uma vez que os grupos precisaram discutir as pistas, formular hipóteses e tomar decisões coletivas para progredir no jogo. Isso favoreceu a participação de todos e tornou o momento mais colaborativo.

Observamos que a proposta conseguiu capturar a atenção dos alunos, especialmente através da narrativa e da divisão em etapas, que proporcionaram um ritmo à atividade. Alguns grupos avançaram com mais facilidade, enquanto outros necessitaram de mais suporte dos mediadores e do chatbot, o que evidenciou que a dinâmica demandava acompanhamento contínuo e mediação ao longo do percurso. Mesmo assim, os alunos permaneceram engajados e demonstraram satisfação ao conseguir superar os desafios apresentados.

Outro resultado significativo foi a percepção de que a atividade contribuiu para a aprendizagem do conteúdo de maneira mais significativa. Ao relacionar as pistas com o tema de phishing, os alunos conseguiram transitar de uma abordagem mais teórica para uma reflexão prática sobre o problema. No final, ficou claro que a experiência não apenas ajudou na compreensão do conteúdo, mas também no desenvolvimento da cooperação entre os grupos e na atenção aos detalhes. Também foi realizada uma enquete no aplicativo “Google Forms”, reunindo o feedback geral da turma.

Como evidenciado pela Figura 3, os resultados da atividade se mostram muito positivos, tendo em vista que obtivemos boas respostas na maioria dos indicadores, sobretudo em aprendizagem, operabilidade e acessibilidade. Como pode ser observado, no item 2 obtivemos 33% das respostas como “Concordo Completamente”, 44% como “Concordo Parcialmente” e 22% como “Indiferentes", evidenciando que a atividade possui uma estética agradável.

Figura 2: Avaliação MEEGA+ (Usabilidade)



Fonte: Elaborado pelos pesquisadores.

Já no item 7, 44% marcou “Concordo Completamente”, 28% “Concordo parcialmente”, 17% “Indiferentes” e apenas 11% escolheu “Discordo Parcialmente”, denunciando bons indicadores no quesito de operacionalidade da atividade e do jogo de investigação. Nessa linha, no item 8 foi possível verificar que 67% afirmou “Concordo Completamente”, 28% “Concordo Parcialmente” e apenas 6% mencionou “Indiferente”, mostrando um bom desempenho da atividade no quesito de acessibilidade.

4 CONSIDERAÇÕES FINAIS

A implementação do jogo Caso Cripto, tanto na forma híbrida apresentada no artigo quanto na perspectiva da aula plugada mencionada, possibilitou solidificar a compreensão de que metodologias ativas, especialmente jogos de investigação, representam uma estratégia pedagógica eficaz para o ensino de conceitos complexos de cibersegurança no ensino médio. Durante este trabalho, foi possível

notar que a abordagem investigativa, combinada com uma narrativa cativante e a organização em etapas progressivas, contribuiu de maneira significativa para o envolvimento dos alunos, promovendo o pensamento crítico, a colaboração e a aplicação prática dos conhecimentos relacionados a tópicos como phishing, envenenamento de DNS e segurança de dados.

Os resultados obtidos mostraram avaliações positivas tanto nos aspectos de usabilidade quanto na percepção de aprendizagem, confiança e relevância do conteúdo. A interação mediada pelo perfil do delegado, utilizando a técnica Wizard of Oz (simulando uma IA), revelou-se eficaz para guiar os grupos sem comprometer o desafio proposto, embora tenha evidenciado a necessidade de um acompanhamento contínuo por parte dos mediadores. A dificuldade enfrentada pelos alunos na fase final do jogo, a descriptografia da senha, ressalta a importância de atividades que demandem raciocínio investigativo e associação criativa de pistas, habilidades essenciais para a formação de usuários críticos no ambiente digital.

5 AGRADECIMENTOS

Agradeço ao orientador e supervisor, pela paciência, dedicação e pelas valiosas orientações. Sua expertise e incentivo foram fundamentais para o amadurecimento das ideias aqui apresentadas e para a conclusão deste trabalho com rigor e qualidade.

Aos coordenadores do PIBID (Programa Institucional de Bolsa de Iniciação à Docência), expresso minha profunda gratidão. A oportunidade de vivenciar o cotidiano escolar e a prática docente através deste programa foi um divisor de águas em minha formação, proporcionando experiências que fundamentaram não apenas este estudo, mas minha identidade como futuro educador.

Ao IFBA Jacobina, pela infraestrutura e pelo corpo docente que contribuíram para o meu crescimento intelectual e profissional durante os anos de graduação.

A CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pelo financiamento através do PIBID o que possibilitou a realização deste trabalho com dedicação e afinco.

REFERÊNCIAS

ARAÚJO, Luis Gustavo. Metodologia IBP3A. In: NO PLUG - IFBA - Computação Desplugada. [S. l.], s.d. Disponível em: https://sites.google.com/view/noplugifba/ibp3a. Acesso em: 24 mar. 2026.

BRASIL. Ministério da Educação. Conselho Nacional de Educação. Parecer CNE/CEB nº 2/2022: Normas sobre Computação na Educação Básica – Complemento à Base Nacional Comum Curricular (BNCC). Brasília, DF: MEC, 2022. Disponível em: https://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file. Acesso em: 27 mar. 2024.

DA SILVA, E. J. A. et al. Observações e reflexões de um jogo criminal utilizando o teorema de tales durante uma experiência com a lesson study. In: Anais do Encontro Nacional de Educação Matemática, 2022.

DA SILVA SOUZA, J. G. ; DOS REIS SILVA, V.; DE JESUS ARAUJO, L. G. P2P unplugged: Uma abordagem de computação desplugada para o ensino de peer-to-peer. In: Escola Regional de Computação Bahia, Alagoas e Sergipe (ERBASE), 2024. p. 365-373.

FARIAS, F. et al. Self Protect: Um jogo para auxílio no ensino de conceitos relacionados a segurança na internet para crianças e adolescentes. In: Anais do XXV Workshop de Informática na Escola, 2019. p. 246-255.

Hassunuma, R. M., Oliveira, A. L. P., Garcia, P. C., & Messias, S. H. N. (2024). COMO UTILIZAR O JOGO MICROMACRO: CRIME CITY NO ENSINO DE CONCEITOS DE BIOMEDICINA FORENSE?. Revista Multidisciplinar De Educação E Meio Ambiente, 5(1), 19–33. https://doi.org/10.51189/integrar/rema/4208.

KELLEY, Jeff; NORMAN, Don; MUNRO, Allen. The Wizard of Oz Method in UX. In: NIELSEN NORMAN GROUP. Fremont, 19 abr. 2024. Disponível em: https://www.nngroup.com/articles/wizard-of-oz/. Acesso em: 24 mar. 2026.

SCHAPPO, B. ; MEDINA, R. Th3Off1c3: um jogo de tabuleiro educacional voltado para o ensino de segurança da informação. 2024. Disponível em: https://teyet-revista.info.unlp.edu.ar/TEyET/article/view/2341. Acesso em: 22 abril 2026.