GAMIFICAÇÃO E APRENDIZAGEM ADVERSARIAL EM CURSOS SUPERIORES DE TECNOLOGIA

GAMIFICATION AND ADVERSARIAL LEARNING IN FLIPPED TECHNOLOGY CLASSROOMS

Hebert de Oliveira Silva[1] , [i]
Jessica Franzon Cruz do Espírito Santo [2], [ii]
Tiago Augusto Orcajo Demay Cordeiro [3], [iii]
Caique Zaneti Kirilo[4], [iv]
Arthur Gustavo de Araujo Ferreira [5], [v]
Vivian de Oliveira Preto [6], [vi]
Emerson Costa Santos[7], [vii]

RESUMO

Este artigo investiga o uso de *gamificação* e de abordagens *adversariais* no ensino de tecnologia, aplicados em projetos integradores e de extensão dos cursos superiores de Segurança Cibernética e Ciência de Dados do SENAI Informática. A proposta pedagógica foi estruturada sob a metodologia de *sala de aula invertida*, combinando elementos de jogos (pontos, níveis, insígnias e *leaderboards*) com desafios de ataque e defesa (por exemplo, *data poisoning* e cenários *red team vs. blue team*) para ampliar engajamento, aprendizagem ativa e pensamento crítico. O estudo de caso analisou o desempenho e a participação dos estudantes em ambiente laboratorial, identificando ganhos em motivação, colaboração e proficiência técnica. Os achados indicam que a integração entre gamificação, abordagens adversariais e sala de aula invertida favorece o desenvolvimento de competências alinhadas às demandas profissionais, embora requeira infraestrutura adequada e mediação docente intensiva.

Palavras-chave: Gamificação; Educação Adversarial; Sala de Aula Invertida; Ciência de Dados; Segurança Cibernética.

ABSTRACT

This article investigates the use of *gamification* and *adversarial* approaches in technology education, applied in integrative and extension projects of the undergraduate programs in Cybersecurity and Data Science at SENAI Informática. The pedagogical proposal was structured under the *flipped classroom* methodology, combining game elements (points, levels, badges, and *leaderboards*) with attack and defense challenges (e.g., *data poisoning* and *red team vs. blue team* scenarios) to enhance engagement, active learning, and critical thinking. The case study analyzed student performance and participation in a laboratory environment, identifying

[1] Doutorando e Docente de Segurança Cibernética na Faculdade SENAI-SP, e-mail: hebert.oliveira@sp.senai.br.
[2] Mestranda e Docente de Ciência de Dados na Faculdade SENAI-SP, e-mail: jessica.santo@sp.senai.br.
[3] Mestre e Docente de Segurança Cibernética na Faculdade SENAI-SP, e-mail: tiago.demay@sp.senai.br.
[4] Doutorando e Docente de Ciência de Dados na Faculdade SENAI-SP, e-mail: caique.zaneti@sp.senai.br.
[5] Doutor e Docente de Ciência de Dados na Faculdade SENAI-SP, e-mail: arthur.ferreira@sp.senai.br.
[6] Mestre e Coordenadora dos cursos superiores de Tecnologia em Ciência de Dados e Segurança Cibernética da Faculdade SENAI-SP, e-mail: vpreto@sp.senai.br.
[7]Doutorando e Diretor do Campus Paulo Antônio Skaf, E-mail: emerson@sp.senai.br

improvements in motivation, collaboration, and technical proficiency. The findings indicate that integrating gamification, adversarial approaches, and the flipped classroom fosters competencies aligned with professional demands, although it requires adequate infrastructure and intensive teacher mediation.

Keywords: Gamification; Adversarial Education; Flipped Classroom; Data Science; Cybersecurity.

1 INTRODUÇÃO

O ensino superior em áreas tecnológicas, como Segurança Cibernética e Ciência de Dados, exige estratégias capazes de acompanhar a evolução dos cenários profissionais e das demandas do mercado. Métodos tradicionais, baseados em exposições teóricas e avaliações centradas em provas escritas, mostram-se limitados diante da necessidade de desenvolver competências práticas, colaborativas e críticas (BERGMANN; SAMS, 2012; BIGGS; TANG, 2011). Nesse contexto, abordagens como gamificação, aprendizagem adversarial e sala de aula invertida têm se consolidado como alternativas promissoras para promover aprendizagem ativa e engajamento.

A *gamificação* aplica elementos de jogos em contextos educacionais (pontos, níveis, insígnias e *leaderboards*) para estimular motivação e tornar a experiência mais dinâmica (DETERDING et al., 2011). A aprendizagem adversarial, inspirada em práticas de *red team vs. blue team* e em ataques/defesas simuladas, desafia os estudantes a explorar vulnerabilidades, projetar contramedidas e refletir sobre os impactos de suas ações (GOODFELLOW; MCDANIEL; PAPERNOT, 2018). A *sala de aula invertida* desloca a absorção de conteúdos teóricos para o estudo prévio, reservando o tempo em sala para atividades práticas e resolução colaborativa de problemas (BERGMANN; SAMS, 2012).

1.1 Problema de pesquisa

Ainda são escassos os estudos que investigam, de forma integrada, o potencial da gamificação e das abordagens adversariais em sala de aula invertida em cursos de tecnologia. Pergunta-se: de que forma a integração entre gamificação, aprendizagem adversarial e sala de aula invertida contribui para o desenvolvimento de competências técnicas e colaborativas em estudantes de cursos superiores de Segurança Cibernética e Ciência de Dados?

1.2 Objetivo(s)

O objetivo geral é analisar o impacto da integração entre gamificação, aprendizagem adversarial e sala de aula invertida na formação de estudantes em tecnologia.
Objetivos específicos:

a) implementar um projeto integrador com base nessas três metodologias;
b) avaliar participação, motivação e desempenho técnico ao longo das atividades;
c) identificar competências desenvolvidas (colaboração, pensamento crítico, resiliência);
d) discutir desafios e limitações da adoção da proposta.

1.3 Justificativa

A integração entre gamificação, sala de aula invertida e aprendizagem adversarial alinha práticas pedagógicas às demandas do mercado, oferecendo desenvolvimento de competências técnicas e socioemocionais de modo prático e contextualizado, além de cobrir lacunas da literatura sobre aplicação simultânea dessas abordagens na educação em tecnologia.

2 REVISÃO DE LITERATURA

A adoção de metodologias ativas no ensino superior tem sido amplamente discutida nas últimas décadas, sobretudo pela necessidade de ampliar engajamento discente e aprendizagem colaborativa. Destaca-se a gamificação como uso de elementos de jogos em contextos não lúdicos, com efeitos positivos sobre motivação e persistência (DETERDING et al., 2011). A sala de aula invertida transfere a exposição teórica para o estudo individual e reserva o tempo de aula para práticas e solução de problemas, ampliando protagonismo discente e o papel mediador do docente (BERGMANN; SAMS, 2012; BIGGS; TANG, 2011).

No campo da segurança cibernética, a aprendizagem adversarial, inspirada em *red team vs. blue team*, demanda domínio técnico, pensamento crítico e colaboração. A exposição a cenários adversariais favorece a compreensão de falhas e estratégias de mitigação (GOODFELLOW; MCDANIEL; PAPERNOT, 2018). Embora os três eixos sejam consolidados isoladamente, há lacunas na literatura quanto à sua integração em um mesmo projeto pedagógico. Combinações com tecnologias emergentes, como IA para avaliação e *feedback* automatizado, têm potencial para ampliar motivação e aprendizagem (HOLMES; BIALIK; FADEL, 2021).

3 METODOLOGIA

A metodologia integrou sala de aula invertida, gamificação e abordagens adversariais em um projeto aplicável aos cursos de Segurança Cibernética e Ciência de Dados do SENAI Informática. No curso de Ciência de Dados, o projeto foi desenvolvido dentro da disciplina de Redes de Computadores e Segurança da Informação, garantindo alinhamento entre a proposta adversarial e os conteúdos curriculares de redes, protocolos e práticas de defesa. O desenvolvimento ocorreu em quatro fases. Na primeira, dedicada ao planejamento do ambiente, os estudantes produziram documentação inicial (arquitetura de rede industrial simulada, inventário de serviços como MQTT, Node-RED, Historian e PLC simulado, e vulnerabilidades intencionais). Na segunda, implementou-se o ambiente funcional em infraestrutura virtualizada, nuvem acadêmica ou laboratório físico, com falhas conhecidas (credenciais fracas, ACLs permissivas, níveis de log verbosos). A terceira fase consistiu em *pentest black box*, por grupos adversários sem conhecimento prévio do alvo, com base em PTES, OWASP IoT e OSSTMM, e ferramentas como Nmap, Wireshark, MQTT Explorer, Metasploit e scripts em Python. Por fim, na quarta fase, consolidaram-se achados em relatório final, com vulnerabilidades exploradas, *flags* e recomendações de mitigação (DETERDING et al., 2011; GOODFELLOW; MCDANIEL; PAPERNOT, 2018; BERGMANN; SAMS, 2012).

A Figura 1 sintetiza as quatro fases, o *backbone* pedagógico (sala invertida, gamificação e adversarial), a avaliação (critérios e resultados) e as salvaguardas (ambiente isolado e mediação docente).

O conteúdo teórico (protocolos industriais, segurança em MQTT e metodologias de *pentest*) foi estudado previamente em materiais digitais; o tempo presencial focou execução prática, discussões e resolução colaborativa. A gamificação ocorreu via pontos, insígnias e *leaderboard*. O componente adversarial envolveu alternância de papéis entre grupos defensores (projeto/entrega do ambiente) e atacantes (execução do *pentest*), promovendo pensamento crítico, antecipação de ameaças e resiliência.

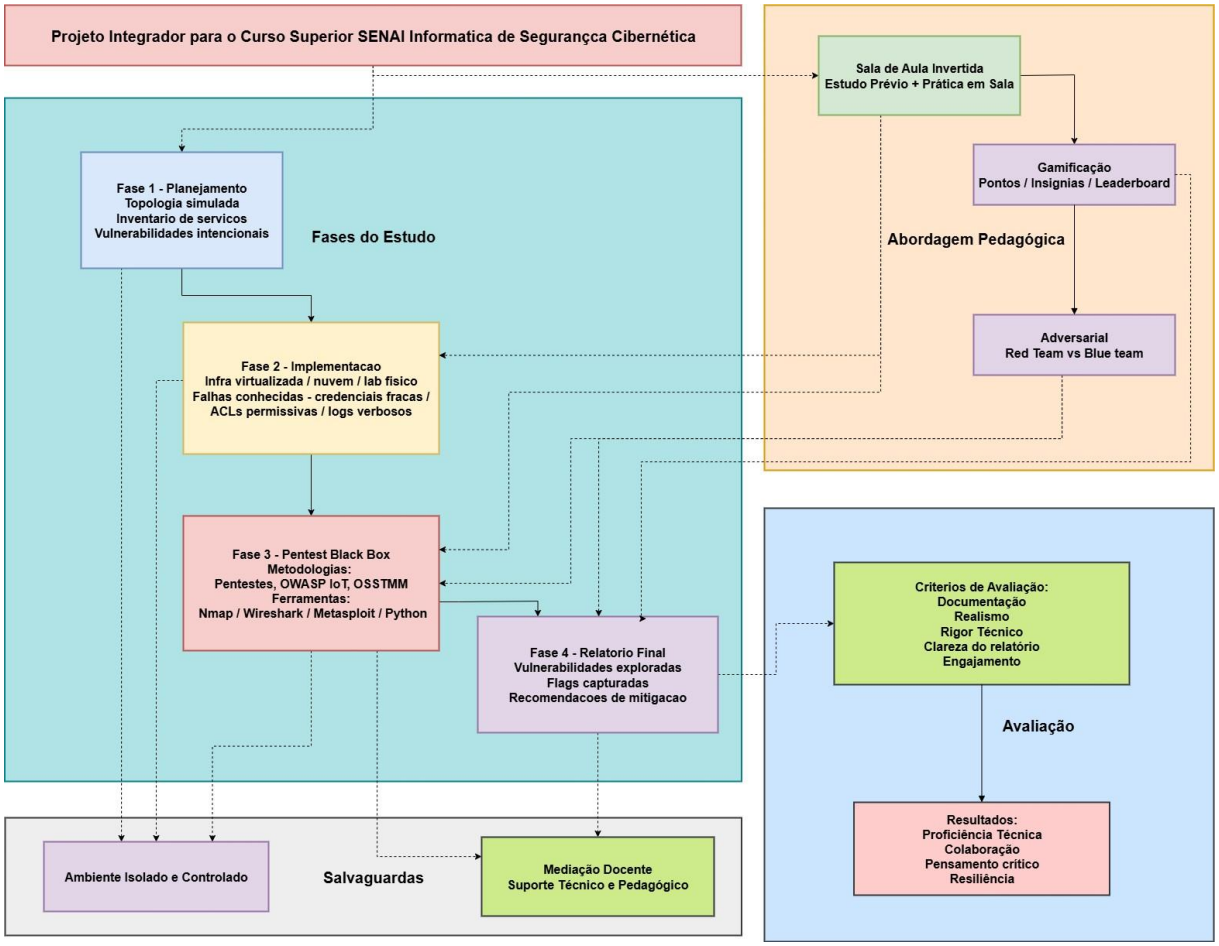

Figura 1 – Metodologia aplicada: fases (P1–P4), abordagem pedagógica, avaliação e salvaguardas. Fonte: elaboração própria com base em (DETERDING et al., 2011; GOODFELLOW; MCDANIEL; PAPERNOT, 2018; BERGMANN; SAMS, 2012).

A avaliação considerou qualidade da documentação e topologia, realismo das vulnerabilidades, rigor metodológico, clareza dos relatórios e engajamento/colaboração. O projeto ocorreu em ambiente isolado e controlado, com mediação docente e falhas propositalmente criadas para fins acadêmicos.

4 RESULTADOS E DISCUSSÕES

A análise dos registros (rubricas, vídeos, observações e artefatos técnicos) indica aumento de engajamento ao longo do projeto. Docentes relataram uso mais intencional do tempo de laboratório e maior colaboração. Discentes, em debriefings, apontaram que metas claras, visibilidade de progresso por leaderboard e problemas autênticos favoreceram motivação e persistência (DETERDING et

al.,2011; BERGMANN; SAMS, 2012).Houve preocupação inicial com a condução do componente adversarial e com regras. Questões sobre fair play, escopo, ética e limites aceitáveis foram tratadas por: i) briefing formal (escopo e limites), ii) código de conduta e checklist, iii) mediação docente durante execuções e post-mortems, preservando benefícios cognitivos das práticas adversariais (GOODFELLOW; MCDANIEL; PAPERNOT, 2018).

Observou-se busca ativa de conhecimento pelos grupos defensores diante de novos vetores de ataque: autenticação no broker MQTT, revisão de ACLs e níveis de log, regras de monitoramento e ajustes de topologia. O movimento ocorreu em momentos síncronos e assíncronos, alinhado ao deslocamento da aquisição conceitual para o estudo prévio e aplicação em sala (BERGMANN; SAMS, 2012). Os estudantes relataram autopercepção de lacunas (redes, Linux, instrumentação de logs, métodos de pentest e protocolos industriais), desencadeando autoestudo e rework orientado por feedback — padrão de aprendizagem autodirigida compatível com a andragogia (KNOWLES; III; SWANSON, 2014) e com o Jeito SENAI de Educar (Serviço Nacional de Aprendizagem Industrial (SENAI), 2019).

Quanto à gamificação, houve ganho de foco e ritmo, com risco pontual de competição excessiva. Mitigações: a) peso maior para qualidade de relatório e eficácia defensiva do que para quantidade de flags; b) pontuação para colaboração intergrupos; c) reforço de dimensões éticas e do propósito formativo. Vídeos de entrega evidenciaram melhora na articulação do raciocínio técnico; rubricas capturaram ganhos em rigor metodológico (planejamento e rastreabilidade) e clareza comunicativa. A triangulação reduziu subjetividade e favoreceu consistência avaliativa (BIGGS; TANG, 2011).

5 CONCLUSÃO

A integração entre sala invertida, gamificação e práticas adversariais, com avaliação por vídeos e rubricas, aproximou teoria e prática, elevou engajamento e fortaleceu protagonismo discente. A preocupação inicial com regras do adversarial foi mitigada por orientações formais e mediação docente, assegurando clareza de escopo e segurança.

Destacou-se a busca ativa de conhecimento e a autopercepção de lacunas, que impulsionaram autoestudo e reexecuções orientadas por feedback — dinâmica andragógica coerente com o Jeito SENAI de Educar (KNOWLES; III; SWANSON, 2014; Serviço Nacional de Aprendizagem Industrial (SENAI), 2019). Como limitações, citam-se o caráter contextual, a heterogeneidade de proficiências e a predominância de evidências qualitativas. Trabalhos futuros incluem delineamentos com grupo controle, diagnósticos e somativos, telemetria de laboratório e calibração de rubricas para equilibrar competição e colaboração, além de explorar feedback automatizado.

REFERÊNCIAS

BERGMANN, J.; SAMS, A. *Flip Your Classroom: Reach Every Student in Every Class Every Day*. [S.l.]: International Society for Technology in Education, 2012. ISBN 978-1564843159.

BIGGS, J.; TANG, C. *Teaching for Quality Learning at University*. 4. ed. [S.l.]: McGraw-Hill Education, 2011. ISBN 978-0335242757.

DETERDING, S. et al. From game design elements to gamefulness: Defining

"gamification". In: *Proceedings of the 15th International Academic MindTrek Conference*. [S.l.]: ACM, 2011. p. 9–15.

GOODFELLOW, I.; MCDANIEL, P.; PAPERNOT, N. Making machine learning robust against adversarial inputs. *Communications of the ACM*, v. 61, n. 7, p. 56–66, 2018.

HOLMES, W.; BIALIK, M.; FADEL, C. *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning*. Paris: UNESCO; Boston: Center for Curriculum Redesign, 2021.

KNOWLES, M. S.; III, E. F. H.; SWANSON, R. A. *The Adult Learner: The definitive classic in adult education and human resource development*. 8. ed. London: Routledge, 2014.

Serviço Nacional de Aprendizagem Industrial (SENAI). *Metodologia SENAI de Educação Profissional*. Brasília: SENAI Departamento Nacional, 2019. Acesso em: today. Disponível em: <https://senaiweb.fieb.org.br/areadocente/assets/Midia/2019/Livro_Msep_2019.pdf>.

AGRADECIMENTOS

À Faculdade SENAI, Direção da Escola SENAI "Antonio Skaf", coordenação, equipe técnica, docentes, estudantes e parceiros institucionais, pelo apoio essencial à realização deste trabalho.

SOBRE O(S)AUTOR(ES)

[i] **Hebert de Oliveira Silva (Autor 1)**

Mestre e Doutorando em Tecnologia da Informação pela UNICAMP; Coordenador de Cibersegurança no Grupo Hapvida e professor (IBMEC, Impacta, UNIP e SENAI Informática). Atuação em Blue/Red Team, governança e resposta a incidentes, com foco em aprendizado federado, IA e segurança em CPS/IoT. Autor de livros e artigos IEEE, ACM e Elsevier.
https://orcid.org/0000-0002-0186-5925

[ii] **Jéssica Franzon Cruz do Espírito Santo (Autor 2)**

Possui graduação (Bacharelado) em Ciência da Computação (2018-2021) pela Universidade Paulista (UNIP); Pós-graduada em Gestão Educacional na Perspectiva Inclusiva (2022) pela Universidade Federal de Pelotas (UFPEL) e Pós-graduada em Psicopedagogia (2024) pela Faculdade das Américas (FAM); É Mestranda em Engenharia da Informação pela Universidade Federal do ABC. Atua como Professora na Faculdade Senai no campus Paulo Antônio Skaf no curso de Ciência de Dados.
https://orcid.org/0000-0002-2812-3673

[iii] **Tiago Augusto Orcajo Demay Cordeiro (Autor 3)**

Mestre em Engenharia de Computação (Poli-USP), pós-graduado em Computação em Nuvem e graduado em Engenharia Eletrônica (IMT). Atua no Insper (Laboratório de Redes e Supercomputação) e como professor de Computação em Nuvem. Pesquisa em redes, segurança com IA e HPC.
https://orcid.org/0000-0002-4991-478

[iv] **Caique Zaneti Kirilo (Autor 4)**

Possui bacharelado em Ciência da Computação (2012-2015); Mestrado em Engenharia de Produção com ênfase em Inteligência Artificial e Seis Sigma na linha de pesquisa de Métodos Quantitativos em Engenharia de Produção focada em Processos decisórios baseados em lógicas não clássicas (2016-2017); É Doutorando em Engenharia da Informação pela Universidade Federal do ABC. Atua como Professor Universitário e Pesquisador integrante do Grupo de Pesquisa de Engenharia de Software aplicada à criação de Sistemas Críticos, atuando também como orientador em programas de iniciação cientifica de alunos da graduação. https://orcid.org/0000-0001-5667-0861

[v] **Arthur Gustavo de Araujo Ferreira (Autor 5)**

Bacharel em Física com ênfase computacional, mestre e doutor em Ciências pela USP. Professor na Escola SENAI de Informática, atua em ciência de dados, inteligência artificial e computação quântica. Tem ampla experiência em Ressonância Magnética Nuclear aplicada ao estudo de meios porosos, computação quântica, petrofísica e materiais cimentícios, com foco em análises de RMN, modelagem estatística e machine learning para caracterização de materiais. Sua carreira integra pesquisa científica, aplicações industriais e ensino.
https://orcid.org/0000-0002-6676-384X

[vi] **Vivian de Oliveira Preto (Autor 6)**

Graduada em Tecnologia Gráfica (Faculdade SENAI Theobaldo de Nigris) e Mestre em Educação (UNESP/Marília). Coordenadora dos cursos superiores de Tecnologia em Ciência de Dados e Segurança Cibernética da Faculdade SENAI Mecatrônica (Campus Paulo Antônio Skaf).
https://orcid.org/0009-0006-0193-5571

[vii] **Emerson Costa Santos (Autor 7)**

Supervisor de Operações do SENAI-SP, com atuação em planejamento, gestão e avaliação de Escolas e Faculdades. Professor Convidado na Sheridan College (Canadá). Doutorando em Sociologia, Mestre em Engenharia Elétrica e Engenheiro Mecânico. Pesquisador no C4AI-USP, CECS-UFABC (Indústria 4.0) e Expert Independente da WorldSkills International. Experiência como especialista e docente em Educação Profissional nas áreas de Manutenção Industrial, Automação, Ferramentaria e EJA.
https://orcid.org/0000-0002-4730-9983