Desafios reais em cibersegurança: uma abordagem educacional em pós-graduação e a importância da parceria com a indústria

Andreia Leles[1], Luciano Freire[1], Rafael Machado[2], Marcelo Parada[2]

[1] Centro Universitário FACENS, Sorocaba – SP – Brasil
[2] Lenovo Tecnologia Brasil, Indaiatuba – SP – Brasil

{andreia.leles, luciano.freire}@facens.br,

rafaelrodrigues.machado@gmail.com,

mparada@lenovo.com

Abstract. *This paper examines the partnership between academia and industry to foster educational innovation in cybersecurity. Real industry challenges bring authenticity to students' learning, enhancing competency development. The proposal, based on challenge- and competency-based learning, was implemented in a postgraduate program. Self-regulated learning supported the evaluation of educational impact. Results indicated the development of competencies recognized by both students and industry. Employability and open innovation validated the model's effectiveness.*

Resumo. *Este artigo analisa a parceria entre academia e indústria para impulsionar a inovação educacional em cibersegurança. Desafios reais do setor trouxeram autenticidade ao aprendizado, promovendo o desenvolvimento de competências. A proposta, baseada em aprendizagem por desafios e competências, foi aplicada em um curso de pós-graduação. A avaliação do impacto educacional baseou-se na aprendizagem autorregulada. Os resultados indicaram o desenvolvimento de competências reconhecidas por alunos e indústria. Empregabilidade e inovação aberta validaram a eficácia do modelo.*

1. Introdução

A demanda por profissionais de Tecnologia da Informação (TI) no Brasil aponta para um *déficit* anual de 106 mil talentos, totalizando 750 mil até 2025 [Brasscom 2025]. Em cibersegurança, a lacuna é ainda maior: 3,4 milhões de profissionais em 2022, com projeção de 85 milhões até 2030 [(ISC)^2 2023, World Economic Forum 2024]. Iniciativas como Hackers do Bem e MCTI do Futuro buscam fomentar a formação de talentos, mas cursos tradicionais ainda enfrentam dificuldades para atender às competências demandadas pela indústria, devido ao ensino focado exclusivamente na transmissão de conteúdos – algo ultrapassado em tempos de inteligência artificial, *Big Data* dentre outras tecnologias que estão revolucionando o mercado de trabalho.

Neste cenário, métodos ativos de aprendizagem ganham destaque, especialmente a *Challenge-Based Learning* (CBL) e a *Competency-Based Education* (CBE), por alinharem ensino e prática profissional [Membrillo-Hernández et al. 2021, Leles et al. 2024].

Nessas abordagens, o aluno torna-se protagonista, e o professor, um facilitador [Kumar et al. 2021, Lee and Shvetsova 2019].

A CBL promove o desenvolvimento de competências por meio de desafios reais, envolvendo mentoria da indústria e integração com outros métodos como *Problem-Based Learning* (PBL), *Project-Based Learning* (PjBL), EpBL *Experencial-Based Learning* e *Scenario-Basead Learning* (SBL) [López-Fernández et al. 2020, Leijon et al. 2022, Leles et al. 2024]. Já a CBE estrutura a aprendizagem por competências técnicas e socioemocionais, enquanto a *Self-Regulated Learning* (SRL) fortalece a autorreflexão do aluno [Henri et al. 2017, Zheng et al. 2020]. Os métodos ativos citados propiciam que o estudante adquira conhecimento, não de forma passiva, mas com a possibilidade de discernir qual a melhor fonte de informação, analisar e compreender os conceitos aprendidos e aplicá-los na solução de um desafio real. Neste contexto, cabe ao docente permitir, identificar e direcionar todas as competências desenvolvidas no processo, alinhando-as a necessidade de mercado.

A análise da aprendizagem pode ocorrer em três momentos: diagnóstica (inicial), formativa (durante o curso) e somativa (por entregas e resultados) [Dolin et al. 2018].

Este estudo investiga como estratégias educacionais fundamentadas na CBL, aliadas à parceria entre instituição de ensino superior (IES) e a indústria, favorecem o desenvolvimento de competências em cibersegurança. As questões de pesquisa são:

- **Q1:** Como analisar a aprendizagem para verificar o desenvolvimento de competências em cibersegurança?
- **Q2:** Quais as vantagens da parceria IES e indústria na viabilização da CBL?

Parte-se da hipótese de que tal colaboração potencializa a aplicação de metodologias ativas, sobretudo a CBL, promovendo o desenvolvimento de competências em contextos reais. A análise da aprendizagem, guiada pela SRL e CBE, permite acompanhar com eficácia o progresso formativo.

Este trabalho propõe uma abordagem educacional baseada na CBL, articulada à parceria estratégica entre a Lenovo e o Centro Universitário FACENS, voltada à formação de especialistas em cibersegurança na pós-graduação *lato sensu*, com foco em contextos reais e tecnologicamente avançados.

A estrutura deste artigo está organizada da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; a Seção 3 descreve a abordagem metodológica adotada; as Seções 4 e 5 detalham, respectivamente, as ações da Lenovo e do Centro Universitário no modelo educacional proposto; a Seção 6 discute os resultados obtidos; e, por fim, a Seção 7 apresenta as considerações finais.

2. Trabalhos Relacionados

A revisão bibliográfica foi guiada pelos temas centrais deste estudo: métodos ativos, parceria com a indústria e cibersegurança. A expressão de busca ((*challenge-based learning* OR *project-based learning* OR *scenario-based learning* OR *competency-based education* OR *competency-based learning*) AND *cybersecurity*) foi aplicada nas bases Web of Science e Scopus, resultando em 46 artigos após remoção de duplicatas.

A maioria dos estudos foca em cursos de graduação, com ênfase em conscientização, treinamentos ou inserção curricular. PjBL e SBL são os métodos mais recorrentes, com pouca colaboração direta com a indústria.

Este estudo se diferencia por: (i) detalhar a atuação conjunta entre IES e indústria; (ii) aplicar a CBL em pós-graduação *lato sensu*; (iii) integrar CBL, CBE e SRL em múltiplas fases avaliativas; e (iv) evidenciar impacto real em empregabilidade, inovação e produção científica.

3. Metodologia

Este estudo é de natureza exploratória e aplicada, conduzido por meio de um estudo de caso instrumental único [Stake 1995], com o objetivo de investigar estratégias educacionais inovadoras em cibersegurança a partir da colaboração entre uma Instituição de Ensino Superior (IES) e uma empresa global de tecnologia.

A opção pelo estudo de caso justifica-se pela necessidade de compreender um fenômeno educacional complexo em seu contexto real [Yin 2015], permitindo uma análise aprofundada de uma intervenção pedagógica singular. A pesquisa, de caráter qualitativo, envolveu uma única IES, a empresa Lenovo e uma turma de pós-graduação (n = 18), sendo 10 alunos participantes voluntários. A metodologia seguiu princípios de rigor científico como coerência metodológica, triangulação de dados e validade ecológica [Merriam 2009]. A Tabela 1 resume a amostra.

Tabela 1. Resumo da amostra e caracterização da empresa parceira

Item	**Descrição**
IES participante	Centro Universitário FACENS, com tradição em Engenharia e Tecnologia.
Turma analisada	1ª turma (início em maio de 2022 e conclusão em abril de 2024), com 18 alunos, sendo 10 voluntários da pesquisa.
Empresa parceira	Lenovo, líder mundial no desenvolvimento e fabricação de tecnologia de ponta, incluindo computadores pessoais, servidores, computadores industriais, *smartphones*, *tablets* e sistemas de *software*. Todos os produtos e soluções passam por rigorosos critérios de segurança (*firmware*, BIOS, software, Linux, *cloud*) e contam com SOC (*Security Operations Center*) em operação 24x7. Os alunos bolsistas mantiveram interação contínua com essas equipes.

O curso analisado adota metodologias ativas amplamente reconhecidas, como *Challenge-Based Learning* (CBL), *Project-Based Learning* (PjBL), *Scenario-Based Learning* (SBL) e *Competency-Based Education* (CBE), aplicadas a desafios reais e inovação aberta.

A coleta de dados foi realizada em duas fases, utilizando um formulário baseado no modelo de *Self-Regulated Learning* (SRL), com foco na percepção dos estudantes sobre competências desenvolvidas e personalização da aprendizagem. A fase 1 caracteriza o período em que os alunos ainda não haviam migrado para realizar as suas atividades na Lenovo. A fase 2 contempla o período em que os alunos já estavam na Lenovo. Os dados

foram complementados por registros institucionais, *feedback* da empresa e indicadores objetivos como empregabilidade, certificações e propostas de patentes. A Tabela 2 detalha as abordagens educacionais e instrumentos de avaliação utilizados.

Tabela 2. Abordagens educacionais e instrumentos de avaliação

Métodos Ativos	**Atividade aplicada**	**Instrumento de avaliação**
CBL	*Hackathon* e TCC baseados em desafios reais da empresa (*open innovation)*.	Avaliação somativa por especialistas (impacto e aplicabilidade).
PjBL	Projetos com metodologias ágeis e inovação aberta.	Avaliação técnica e produção científica.
SBL	*Bootcamp* com simulações e estudos de caso.	Observação estruturada e autoavaliação (SRL).
CBE + SRL	Ciclo formativo completo (nivelamento, mentorias e desafios).	Formulário baseado em SRL e autoavaliação de competências. Pesquisa realizada com alunos em duas fases: antes (fase 1) e depois (fase 2) de migrarem para as instalações e projetos reais da Lenovo.

A análise dos dados seguiu os princípios da CBE e SRL, com categorias temáticas relacionadas às competências desenvolvidas, sua aplicabilidade e o impacto da proposta pedagógica. As inferências foram tratadas com foco na transferibilidade para contextos similares, reconhecendo as limitações de generalização estatística.

A pesquisa respeitou os princípios éticos estabelecidos pela legislação brasileira, com garantia de anonimato e conformidade com a Lei Geral de Proteção de Dados (LGPD). A coleta teve finalidade exclusivamente científica e pedagógica.

Para reforçar a validade dos achados, a triangulação metodológica [Guba and Lincoln 1989] foi aplicada com três fontes principais: (i) formulários baseados em SRL/CBE [Zheng et al. 2020, Henri et al. 2017]; (ii) análise documental dos projetos e atividades realizadas na IES e Lenovo; (iii) indicadores objetivos (certificações, projetos em uso, propostas de patentes). Essa estratégia fortaleceu a validade ecológica [Merriam 2009], garantindo aderência ao contexto real da formação e reforçando o potencial de replicabilidade da abordagem em programas de formação em cibersegurança.

4. Programa Educacional – Ações da Indústria (Lenovo)

Por meio de seu programa de P&D e responsabilidade social, a Lenovo propôs uma pós-graduação em cibersegurança, oferecendo bolsas integrais para atuação de 20h semanais em projetos reais. Professores e especialistas também foram remunerados. A iniciativa foi viabilizada via Lei da Informática e nomeada internamente Projeto Connor.

Na primeira edição, participaram duas universidades e a FACENS, credenciada como Instituição Científica, Tecnológica e de Inovação (ICT), com 10 alunos selecionados por instituição, totalizando 30 bolsistas. As IES criaram seus cursos com apoio da Lenovo na definição de ementas e disciplinas conforme demandas do setor.

A Lenovo ofereceu mentoria técnica, apoio a laboratórios, materiais didáticos e a vivência dos bolsistas em sua estrutura organizacional, caracterizada como Laboratório Vivo de Aprendizagem (LVA). Essa imersão, tratada como *onboarding*, inseriu os estudantes em desafios corporativos reais.

O programa incluiu processos seletivos internos, reuniões quinzenais entre IES e empresa, e encontros presenciais trimestrais com especialistas. Dois entregáveis principais foram definidos: (i) TCC individual por IES; e (ii) *hackathon* interinstitucional, com equipes mistas para portfólios, identificação de talentos e soluções inovadoras.

5. Programa Educacional – Ações do Centro Universitário FACENS

Este estudo foca na implementação do programa pela FACENS, situada no interior paulista. A proposta educacional foi estruturada com base em CBL, PjBL, CBE e SRL, considerando as demandas da empresa parceira, diretrizes internacionais [Burley et al. 2017] e a Política Nacional de Cibersegurança [Brasil 2023].

Com duração de 24 meses e 440 horas, o curso é composto por quatro módulos: fundamentos, redes e sistemas, *hardening* e normas, e tecnologias emergentes (IA, *blockchain*). Um módulo paralelo de nivelamento prepara alunos de diferentes formações em conteúdos como programação, arquitetura de computadores e *Internet of Things* (IoT).

Ao fim de cada módulo, os estudantes enfrentam um *bootcamp* com foco em competências reais. O TCC é desenvolvido em formato de *open innovation*, com banca mista. São aplicadas estratégias de CBL integradas com outros métodos ativos como SBL, ExBL e PjBL, com metodologias ágeis (Scrum, Lean Startup).

Os cursos de nivelamento (10 a 25h) viabilizam a inclusão de alunos de engenharia elétrica e mecatrônica, por exemplo, com foco em segurança de *hardware* e *firmware*. Cada curso termina com desafio em cenários (SBL) e gestão ágil.

A coordenação do curso é dividida entre um docente técnico em cibersegurança e outro em inovação e projetos, garantindo alinhamento entre conteúdo, metodologias ativas e gestão por competências, além da interface com a empresa.

O *hackathon* institucional estimula inovação e identificação de talentos. Com duração de 30 dias, envolve *workshops* temáticos, *Design Thinking* e ciclos Scrum, gerando *Minimum Product Viable* (MVP) avaliados por especialistas e compondo o portfólio dos alunos.

Em síntese, estruturou-se um modelo educacional baseado em desafios reais, forte integração com a indústria e personalização do processo formativo, promovendo competências técnicas e socioemocionais com avaliação contínua por competências.

6. Resultados e Discussões

Esta seção apresenta os resultados quantitativos e qualitativos que respondem às questões de pesquisa. A análise considera duas fases: o 6º mês (Fase 1) e o 17º mês (Fase 2),

integrando percepções dos alunos, desempenho em desafios, empregabilidade e inovação.

6.1. Percepção dos Alunos e Desenvolvimento de Competências

Os dados quantitativos obtidos por meio de questionários (Tabela 3 e Figura 1) revelam alto índice de satisfação com o curso (Q4 e Q7) e intenção de permanência na área (Q3 e Q5). A menor média (Q6) indica oportunidade de aprimoramento na integração entre teoria e prática. As respostas foram trianguladas com registros institucionais, reflexões dos alunos e *feedback* da empresa parceira, confirmando o alinhamento da proposta com CBE e SRL. A Figura 2 apresenta as competências mais citadas espontaneamente pelos alunos, por autorreflexão.

Tabela 3. Médias das respostas dos alunos (mês 6 e 17)

Cód.	Questão	Mês 6	Mês 17
Q1	Módulo 1 colaborou com atividades na Lenovo?	3,5	–
Q2	Módulo 2 colaborou com atividades na Lenovo?	3,4	–
Q3	Intenção de continuar na área após o curso	4,8	–
Q4	Recomendaria a pós-graduação	4,9	–
Q5	Importância da atuação na Lenovo	–	4,6
Q6	Sinergia entre atividades na Lenovo e a Pós	–	3,5
Q7	Recomendação geral do Programa	–	5,0

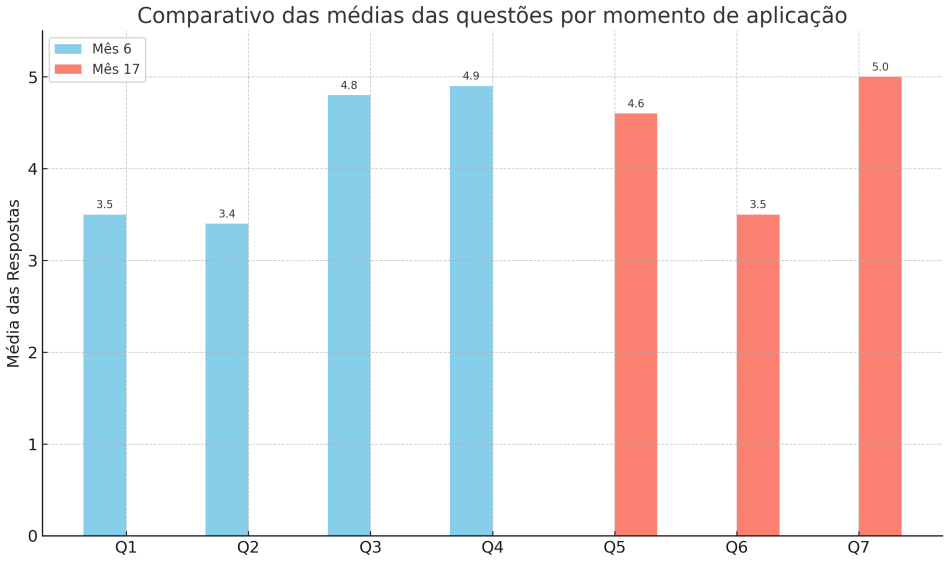

Figura 1. Avaliação dos alunos (mês 6 e 17)

6.2. Hackathon, Inovação e Talentos

O hackathon contribuiu para o desenvolvimento técnico e interpessoal dos estudantes. Foram propostos 9 desafios envolvendo *ransomware*, *phishing*, IoT e computação quântica. As soluções, elaboradas com apoio de especialistas e conduzidas por ciclos de *Design Thinking*, foram avaliadas por uma banca multidisciplinar. As três melhores foram premiadas em evento institucional com a presença da alta gestão da IES e da Lenovo.

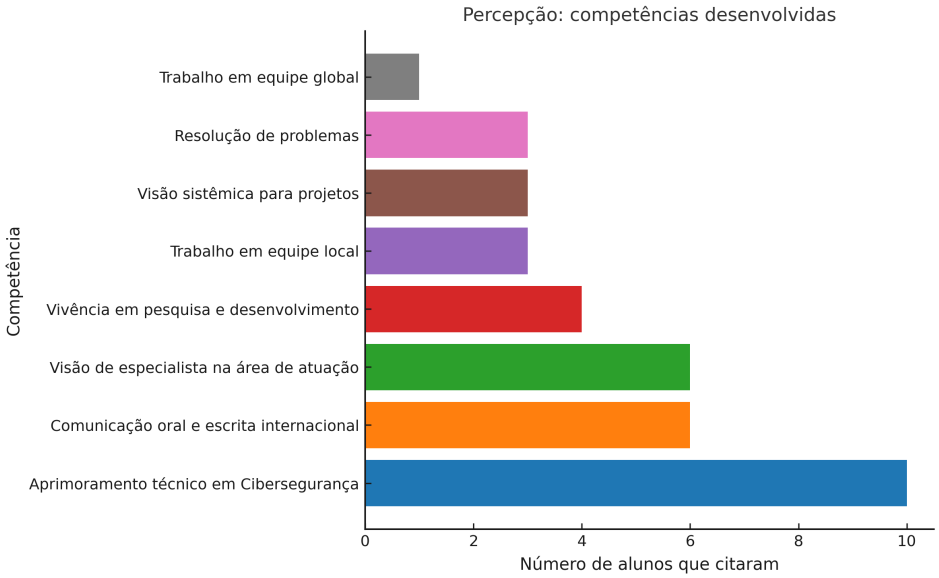

Figura 2. Competências mais desenvolvidas (percepção dos alunos)

6.3. Impacto da Parceria Acadêmica e Indústria

A Figura 3 mostra a avaliação das atividades educacionais, com destaque para *bootcamps*, nivelamento e TCC. A validação de projetos e participação da empresa parceira nas bancas reforçaram o engajamento dos alunos e o alinhamento ao mercado.

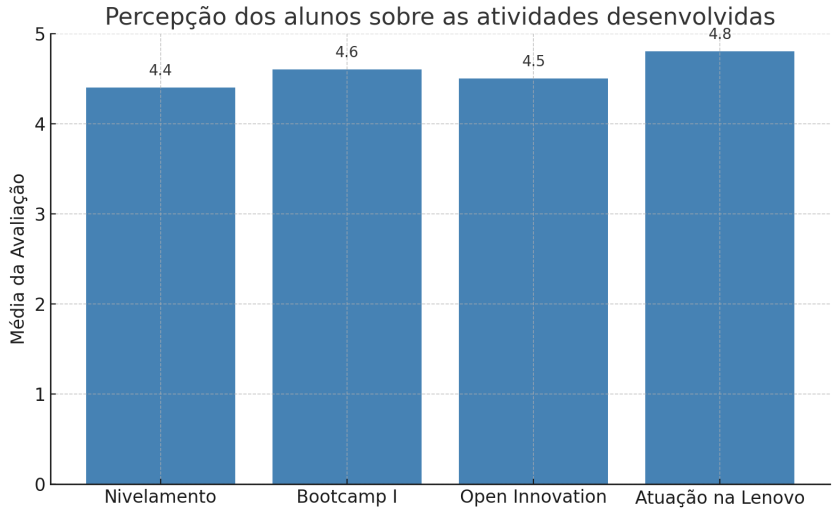

Figura 3. Avaliação dos alunos sobre as atividades formativas

A Tabela 4 resume os principais indicadores de impacto da formação. Os dados indicam que o modelo educacional baseado em CBL, SRL e parceria com a indústria gerou impacto positivo para os alunos e para a empresa. Destacam-se: empregabilidade, inovação e reconhecimento institucional. A replicação futura do modelo já está em curso por meio de turma *in company*, formada em 2025 e início da 2ª turma em setembro de 2024.

Tabela 4. Indicadores de impacto observados

Indicador	**Descrição e Evidência**
Empregabilidade	100% empregados; 70% contratados pela Lenovo.
Certificações técnicas	Certificações relevantes conquistadas durante o curso.
Produção científica	4 artigos no Bootcamp e 10 soluções no TCC.
Registro de patentes	Um projeto em processo de patente com a Lenovo.
Escalabilidade	Nova turma com apoio do MCTI e expansão institucional.

7. Considereções Finais

Este estudo confirmou a hipótese de que a parceria entre IES e indústria, com base em metodologias ativas como CBL, CBE e SRL, é eficaz no desenvolvimento de competências em cibersegurança. A proposta educacional gerou resultados expressivos, como empregabilidade, certificações, produção científica e inovação, incluindo um pedido de patente.

A análise da aprendizagem baseada em SRL e CBE permitiu um acompanhamento reflexivo e orientado a competências, promovendo engajamento e alinhamento entre objetivos acadêmicos e demandas do setor produtivo. O uso do Laboratório Vivo de Aprendizagem (LVA) e do *hackathon* como recursos formativos demonstrou alto potencial para aplicação prática e identificação de talentos.

Apesar dos resultados positivos, destaca-se a necessidade de replicação do modelo em novas turmas para avaliar sua eficiência em diferentes contextos. A continuidade do programa pela Lenovo, com turmas *in company* e apoio do MCTI, indica a escalabilidade e a consolidação institucional da proposta.

Como trabalhos futuros, recomenda-se: (i) explorar a aplicação do modelo em formatos híbridos ou a distância, ampliando o acesso à formação especializada; (ii) adaptar o currículo às regulamentações emergentes em cibersegurança, como o *Cyber Resilience Act* e a *EU Radio Equipment Directive* [Mueck et al. 2025], considerando que a crescente demanda por profissionais da área será impulsionada por exigências legais relacionadas à segurança e privacidade digital.

Agradecimentos

Esse projeto de capacitação foi financiado pela Lenovo, sob investimento da Lei de Informática, MCTI.

Referências

Brasil (2023). Decreto nº 11.856, de 26 de dezembro de 2023. Diário Oficial da União: seção 1, Brasília, DF, ed. extra, p. 1, 26 dez. 2023. Institui a Política Nacional de Cibersegurança - PNCiber e cria o Comitê Nacional de Cibersegurança - CNCiber.

Brasscom (2025). Estudo da brasscom aponta demanda de 797 mil profissionais de tecnologia até 2025. Acesso em: 07 abr. 2025.

Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Hawthorne, E., and Buck, S. (2017). Acm joint task force on cybersecurity education. In *Proceedings of the 2017 ACM SIGCSE technical symposium on computer science education*, pages 683–684.

Dolin, J., Black, P., Harlen, W., and Tiberghien, A. (2018). Exploring relations between formative and summative assessment. *Transforming assessment: Through an interplay between practice, research and policy*, pages 53–80.

Guba, E. G. and Lincoln, Y. S. (1989). *Fourth Generation Evaluation*. Sage Publications, Newbury Park, CA.

Henri, M., Johnson, M. D., and Nepal, B. (2017). A review of competency-based learning: Tools, assessments, and recommendations. *Journal of engineering education*, 106(4):607–638.

(ISC)^2 (2023). Cybersecurity workforce study: Looking deeper into the workforce gap. Acesso em: 07 abr. 2025.

Kumar, A., Krishnamurthi, R., Bhatia, S., Kaushik, K., Ahuja, N. J., Nayyar, A., and Masud, M. (2021). Blended learning tools and practices: A comprehensive analysis. *IEEE ACCESS*, 9:85151–85197.

Lee, J. H. and Shvetsova, O. A. (2019). The impact of vr application on student's competency development: A comparative study of regular and vr engineering classes with similar competency scopes. *SUSTAINABILITY*, 11.

Leijon, M., Gudmundsson, P., Staaf, P., and Christersson, C. (2022). Challenge based learning in higher education–a systematic literature review. *Innovations in education and teaching international*, 59(5):609–618.

Leles, A., Zaina, L., and Cardoso, J. R. (2024). Challenge-based learning for competency development in engineering education, a prisma-based systematic literature review. *IEEE Transactions on Education*.

López-Fernández, D., Sánchez, P. S., Fernández, J., Tinao, I., and Lapuerta, V. (2020). Challenge-based learning in aerospace engineering education: the esa concurrent engineering challenge at the technical university of madrid. *Acta Astronautica*, 171:369–377.

Membrillo-Hernández, J., de Jesús Ramírez-Cadena, M., Ramírez-Medrano, A., García-Castelán, R. M., and García-García, R. (2021). Implementation of the challenge-based learning approach in academic engineering programs. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, 15(2):287–298.

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation*. Jossey-Bass.

Mueck, M., Roberts, T., Du Boispéan, S., and Gaie, C. (2025). Introduction to the european cyber resilience act. In *European Digital Regulations*, pages 91–110. Springer.

Stake, R. E. (1995). *The Art of Case Study Research*. SAGE Publications.

World Economic Forum (2024). There aren't enough cybersecurity workers. a new report explains why. Acesso em: 07 abr. 2025.

Yin, R. K. (2015). *Case Study Research and Applications: Design and Methods*. SAGE Publications, 6 edition.

Zheng, J., Xing, W., Zhu, G., Chen, G., Zhao, H., and Xie, C. (2020). Profiling self-regulation behaviors in stem learning of engineering design. *Computers & Education*, 143:103669.