Uma Análise Quali-Quantitativa sobre o Engajamento dos Usuários de uma Plataforma Gamificada para Treinamento em Resposta à Incidentes

Alvaro Santana Santos[1], **Rodrigo Sanches Miani**[1], **Rafael Dias Araújo**[1]

[1] Faculdade de Computação (FACOM) – Universidade Federal de Uberlândia (UFU)

{alvaro.santana,miani,rafael.araujo}@ufu.br

Abstract. *This article evaluates the motivation and intention to use a gamified learning platform aimed at teaching cybersecurity incident handling and response, with scenarios based on anonymized real-world incidents (Learn from Incidents - LFI). The evaluation, conducted with 35 residents of the Hackers do Bem technological training and residency program from RNP (Rede Nacional de Ensino e Pesquisa), employed a mixed-methods approach based on the UTAUT model operationalized via PLS-SEM and qualitative analyses of feedbacks. The results indicated good platform acceptance, with means above 4.0 in the constructs of Performance Expectancy, Effort Expectancy, and Behavioral Intention. Effort Expectancy was the main predictor of intention to use (β = 0.325), followed by Social Influence (β = 0.204), and the model explained 48.4% of the variance in behavioral intention (R^2 = 0.484). Furthermore, three of the four learning tracks achieved approval rates above 80.0%. The results highlight the potential of the LFI as an educational tool for specialized training in cybersecurity incident handling and response.*

Resumo. *Este artigo avalia a motivação e a intenção de uso de uma plataforma gamificada de aprendizagem voltada ao ensino de tratamento e resposta a incidentes de cibersegurança com cenários baseados em incidentes reais anonimizados (Learn from Incidents - LFI). A avaliação, conduzida com 35 residentes do programa de formação e residência tecnológica Hackers do Bem da RNP(Rede Nacional de Ensino e Pesquisa), utilizou abordagem quali-quantitativa baseada no modelo UTAUT operacionalizado via PLS-SEM e análises qualitativas de feedbacks. Os resultados indicaram boa aceitação da plataforma, com médias superiores a 4,0 nos constructos de Expectativa de Desempenho, Expectativa de Esforço e Intenção Comportamental. A Expectativa de Esforço foi o principal preditor da intenção de uso (β = 0,325), seguida pela Influência Social (β = 0,204), e o modelo explicou 48,4% da variância da intenção comportamental (R^2 = 0,484). Além disso, três das quatro trilhas obtiveram taxas de aprovação superiores a 80,0%. Os resultados evidenciam o potencial da LFI como ferramenta educacional para capacitação especializada em tratamento e resposta a incidentes.*

1. Introdução

A cibersegurança é uma preocupação atual em diversos setores da sociedade, impulsionada pela proliferação de dispositivos conectados, e pelo uso crescente de inteligência artificial para fraudes e invasões. Esse cenário exige profissionais com habilidades técnicas

e comportamentais para uma resposta adequada a incidentes. Segundo o estudo da ISC2 (*International Information System Security Certification Consortium*), existem 5,5 milhões de profissionais atuando na área globalmente, mas a lacuna de 4,8 milhões indica que quase 47% da demanda mundial não está sendo atendida, e enquanto o número de profissionais permaneceu praticamente estável, essa lacuna cresceu 19% em um único ano, evidenciando uma demanda crescente por formação qualificada que governos e empresas buscam suprir (ISC2 2024). Em paralelo, a gamificação tem emergido como uma estratégia promissora para engajar usuários no contexto da cibersegurança. Elementos como pontos, níveis e intervalos de tempo oferecem *feedback* imediato e simulam a urgência característica de cenários reais de ameaça (Sodikin and Hikmawan 2023). Recompensas e indicadores de progressão, como *badges* e *leaderboards*, têm sido incorporados a plataformas de treinamento para manter o engajamento contínuo e criar uma percepção clara de evolução por parte do usuário (Ashley et al. 2022; Shahzadi et al. 2025).

A partir de uma busca exploratória de plataformas de ensino em cibersegurança, identificou-se um ecossistema diversificado que atende desde iniciantes até profissionais especializados, com destaque para TryHackMe (TryHackMe 2026), HackTheBox (HackTheBox 2026), Cybrary (Cybrary 2026) e, no contexto brasileiro, a Escola Virtual Gov (ENAP 2026) e o IBSEC (IBSEC 2026). Contudo, a maior parte dessas plataformas foi concebida para o desenvolvimento contínuo de profissionais já inseridos na área, sem mecanismos explícitos de avaliação do engajamento. Poucas oferecem trilhas dedicadas, estruturadas e progressivas voltadas especificamente à triagem e resposta a incidentes.

Nesse cenário, a Rede Nacional de Ensino e Pesquisa (RNP), organização social vinculada ao Ministério da Ciência, Tecnologia e Inovações, promove por meio do Programa Hackers do Bem, desenvolvido em parceria com a *Softex* e o Senai-SP, iniciativas voltadas à formação avançada em cibersegurança para suprir a crescente demanda por profissionais qualificados. Neste contexto, emerge a iniciativa GT-LFI (*Learn From Incidents*) (GT-LFI – Learning From Incidents 2026). O projeto estrutura-se em quatro módulos complementares, ANON-LFI que é uma ferramenta de anonimização de incidentes, o *Insight-LFI* que é um motor de IA para categorização automática de incidentes, o módulo *Validate-LFI* que é uma ferramenta de gestão de incidentes e geração de *playbooks* e o Módulo *Learn-LFI* que é o núcleo central deste trabalho. Este módulo implementa uma GLP (*Gamified Learning Platform*) com conteúdo estruturado e com cenários práticos baseados em incidentes reais de cibersegurança. A plataforma propõe proporcionar uma experiência educacional contextualizada onde estudantes desenvolvem competências técnicas e habilidades de tomada de decisão em tratamento e resposta a incidentes (T&RI).

A avaliação de plataformas gamificadas exige compreender como seus elementos influenciam a percepção e o comportamento do usuário. A aceitação tecnológica consolidou-se como um método amplamente utilizado para mensurar variáveis como utilidade percebida e intenção de uso (Bayır and Akel 2024). No contexto educacional, indicadores comportamentais como engajamento, participação e taxa de conclusão também devem ser considerados, uma vez que a simples aplicação de mecânicas de jogo não garante, por si só, o aumento da motivação ou do desempenho (Lopes et al. 2024).

Este trabalho tem como objetivo geral avaliar a motivação e a intenção de uso de uma plataforma gamificada voltada ao treinamento em resposta e tratamento de in-

cidentes de segurança, buscando compreender como os usuários percebem e aceitam a plataforma em seu processo de aprendizagem. Para isso, adotou-se uma abordagem quali-quantitativa, respondendo à seguinte pergunta de pesquisa: *em que medida uma plataforma educacional gamificada influencia a motivação e a intenção de uso contínuo de seus usuários no contexto de resposta e tratamento a incidentes de segurança?*

Como contribuição científica, este trabalho investiga a aceitação e a intenção de uso de uma plataforma gamificada para treinamento em resposta a incidentes de cibersegurança, área ainda pouco explorada na literatura de tecnologias educacionais, combinando métodos quantitativos e qualitativos. Como contribuição técnica, a proposta detalha trilhas práticas fundamentadas em incidentes reais relacionados a ataques distribuídos de negação de serviço (DDoS, do inglês *Distributed Denial of Service*) anonimizados. No âmbito social, contribui para a formação de profissionais em cibersegurança, alinhando-se ao ODS 4 (Organização das Nações Unidas 2015) e aos Grandes Desafios da Computação no Brasil 2025–2035 (Sociedade Brasileira de Computação 2025).

2. Arcabouço Conceitual

2.1. Gamificação

Gamificação é o uso de mecanismos e dinâmicas de jogos para motivar e engajar indivíduos (Busarello 2016). Elementos como pontos, níveis, recompensas e *feedback* imediato estimulam a dedicação do usuário e favorecem a imersão em ambientes de aprendizado, tornando tarefas complexas mais atrativas e significativas. Na cibersegurança, a gamificação costuma ser aplicada em treinamentos corporativos com simulações de *phishing* e certificações por níveis, no ensino superior por meio de laboratórios virtuais e competições CTF (*Capture The Flag*), e no desenvolvimento profissional com *serious games*. (Khoo and Johnkhan 2017) demonstraram que jogos tornam a experiência mais positiva e envolvente para os participantes, aplicando seus elementos diretamente aos treinamento de cibersegurança, como simulações gamificadas e exercícios interativos.

2.2. Avaliação de Aceitação Tecnológica - UTAUT

A Teoria Unificada de Aceitação e Uso de Tecnologia (UTAUT, do inglês *Unified Theory of Acceptance and Use of Technology*) (Venkatesh et al. 2003) integra oito modelos de aceitação tecnológica em quatro constructos principais: Expectativa de Desempenho (PE), Expectativa de Esforço (EE), Influência Social (SI) e Condições Facilitadoras (FC). O modelo também considera gênero, idade, experiência e voluntariedade como moderadores dessas relações (Al-Momani and Ramayah 2025). Em contextos educacionais, EE e SI tendem a influenciar a intenção de uso, enquanto PE se destaca em ambientes organizacionais (Attuquayefio and Addo 2014). A Intenção Comportamental (BI), por sua vez, é o principal preditor do uso efetivo da tecnologia (Al-Momani and Ramayah 2025; Olaniyi 2025). Assim, o UTAUT é adequado para avaliar a aceitação de plataformas web gamificadas e os fatores que condicionam sua adoção e continuidade de uso.

A avaliação das propriedades psicométricas dos constructos é uma etapa fundamental na validação de modelos de pesquisa que utilizam instrumentos de medição baseados em escalas (Almaiah et al. 2019). Três indicadores são amplamente empregados para essa finalidade: o Alfa de Cronbach (α), a Confiabilidade Composta (ρ_c) e a Variância

Média Extraída (AVE). O Alfa de Cronbach mede a consistência interna entre os itens de um mesmo constructo. A Confiabilidade Composta é uma medida mais robusta que o α, pois leva em conta as cargas fatoriais individuais de cada indicador. A AVE expressa a proporção média da variância dos indicadores explicada pelo constructo latente. A utilização dessas análises é necessária para validar que as inferências estatísticas derivadas do modelo estrutural sejam válidas e confiáveis para os resultados obtidos.

Partial Least Squares Structural Equation Modeling (PLS-SEM) é uma técnica estatística que permite estimar simultaneamente relações complexas entre múltiplas variáveis dependentes e independentes, que pressupõem estruturas simples, variáveis diretamente observáveis e a ausência de erros de mensuração (Hair et al. 2021). Diferentemente da abordagem baseada em covariância (CB-SEM), o PLS-SEM adota uma perspectiva preditiva e orientada à maximização da variância explicada nos constructos dependentes, sem exigir normalidade multivariada dos dados e sendo especialmente adequado para amostras de tamanho reduzido e modelos complexos.

2.3. Análise de Sentimentos baseada em Lexicon

A análise de sentimentos baseada em léxico (*lexicon-based sentiment analysis*) é uma abordagem de Processamento de Linguagem Natural que classifica textos segundo sua polaridade semântica (positiva, negativa ou neutra) sem necessidade de corpus de treinamento, utilizando léxicos nos quais palavras ou expressões recebem valores de polaridade previamente atribuídos (Khoo and Johnkhan 2018). Diferentemente das abordagens de aprendizado de máquina, que requerem grandes conjuntos de dados anotados para treinar classificadores, o método léxico aplica diretamente uma fórmula de agregação sobre os valores de polaridade das palavras identificadas no texto, que realiza a diferença entre a contagem de palavras positivas e negativas, normalizada pelo comprimento do documento, e produz um resultado numérico de sentimento por resposta.

2.4. Referenciais de formação em cibersegurança

Com base nos Referenciais de Formação da Sociedade Brasileira de Computação (SBC) (Zorzo et al. 2017), os currículos de Ciência da Computação, Engenharia de Computação, Engenharia de Software e Sistemas de Informação tratam a segurança de forma predominantemente preventiva e voltada ao projeto de sistemas seguros. Conteúdos específicos de resposta a incidentes — como triagem, análise forense, contenção, recuperação e gestão de equipes CSIRT/CERT — não são contemplados, evidenciando uma lacuna na formação dos egressos. O Bacharelado em Cibersegurança (SBC 2023), por sua vez, contempla esses conteúdos em eixos de Segurança de Sistemas e Segurança Organizacional. Contudo, por ainda não integrar as Diretrizes Curriculares Nacionais e ser considerado um curso emergente, sua oferta permanece pouco representativa diante dos cursos tradicionais. Assim, a formação específica em resposta a incidentes ainda alcança um número reduzido de egressos no Brasil.

3. Trabalhos Relacionados

Na área de educação em cibersegurança, diversas plataformas incorporam elementos de gamificação que referenciam o desenvolvimento de novas soluções. Para iniciantes, SpaceShelter (Google 2026b) e Google Interland (Google 2026a) adotam narrativas imersivas com *feedback* imediato. No segmento de e-learning, Coursera, Udemy, Cybrary e

Alura oferecem cursos estruturados com progressão e desafios práticos. Em ambientes de simulação, KC7Cyber (KC7 Cyber 2026), Bandit (OverTheWire 2026) e TryHackMe (TryHackMe 2026) disponibilizam desafios progressivos que aproximam a experiência de situações reais. No âmbito acadêmico, estudos como (Mostafa and Faragallah 2019; Karagiannis and Magkos 2021; Thombre and Velankar 2022; Ashley et al. 2022) apresentam *serious games* e plataformas CTF para ensino de segurança, enquanto (Pirta-Dreimane et al. 2024) propõem um *escape room* híbrido cobrindo o ciclo completo de resposta a incidentes segundo o NIST SP 800-61.

Diante desse panorama, sintetizado na Tabela 1, este trabalho avalia uma GLP (*Gamified Learning Platform*) que combina gamificação com cenários baseados em incidentes reais anonimizados de ataques DDoS, utilizando o modelo UTAUT para preencher uma lacuna identificada na literatura quanto à avaliação de plataformas voltadas ao tratamento e resposta a incidentes.

Tabela 1. Trabalhos discutidos sobre Gamificação, Educação e Cibersegurança.

Referência	**Objeto de Estudo**	**Área de Cibersegurança**	**Aplicação para Tratamento e Resposta a Incidentes**	**Método de Avaliação**
Mostafa & Faragallah (2019)	Seis *serious games* (simulação, RPG, puzzle, quiz etc.) para ensino de segurança da informação.	Ataques de rede, segurança web, engenharia social e políticas de segurança.	–	Pré/pós-teste com ANOVA; questionário Likert.
Karagiannis & Magkos (2021)	Plataforma CTF com desafios de enumeração, ataques de senha e *reverse shell*.	Redes, protocolos e ataques.	–	*Pre-engagement survey*.
Ashley et al. (2022)	Plataforma CTF para ICS, *Smart Grids* e SCADA.	Sistemas de Controle Industrial e infraestruturas críticas.	Simulação de ataques e defesa em infraestruturas críticas.	Tempo de conclusão e precisão.
Thombre & Velankar (2022)	Jogos criados por estudantes com base na tríade CIA.	Redes, protocolos e ataques.	–	Feedback qualitativo.
Pirta-Dreimane et al. (2024)	*Escape room* híbrido com equipes no papel de CSIRT do setor energético.	Resposta a incidentes, DoS, *phishing* e infraestrutura crítica.	Ciclo completo NIST SP 800-61: detecção, contenção, recuperação e comunicação de crise.	Pontuação, questionários psicológicos e autoavaliação pré/pós.
OverTheWire – Bandit (2026)	*Wargame* online com 34 níveis progressivos via SSH para iniciantes.	Linux, SSH, permissões e criptografia básica.	–	Progressão implícita por níveis.
Cybrary (2026)	LMS especializado com trilhas alinhadas ao NICE/NIST para profissionais e equipes corporativas.	Resposta a incidentes, forense, SOC e certificações (CEH, CISSP).	Trilha de *Incident Handler*: detecção, contenção e recuperação com labs práticos.	XP, badges, certificados e relatórios de progresso.
KC7Cyber (2026)	Plataforma gratuita de investigação de incidentes onde o aprendiz atua como analista de SOC.	Análise de logs, detecção de intrusões e investigação forense.	Simulação de incidentes reais (ransomware, movimento lateral) via KQL.	*Scoreboard* em tempo real e métricas de progressão.

Continua na próxima página...

Tabela 1 – Continuação da página anterior

Referência	Objeto de Estudo	Área de Cibersegurança	Aplicação para Tratamento e Resposta a Incidentes	Método de Avaliação
TryHackMe (2026)	Plataforma com +500 labs e CTFs organizados em trilhas estruturadas.	Pentest, redes, forense e segurança defensiva.	–	Pontos, badges, *leaderboards* e certificados.
LMS Generalistas (2026)	Plataformas de e-learning (Coursera, edX, Udemy, Alura) com cursos variados de cibersegurança.	Segurança geral, redes e tópicos introdutórios.	–	Questionários, projetos e certificados de conclusão.
Este trabalho (2026)	GLP com pontos, progressão, badges, avatares e moeda virtual.	Tratamento e resposta a incidentes e ataques DDoS (Python).	Incidentes reais anonimizados de DDoS com tomada de decisão e mitigação.	Análise Quali-Quantitativa com UTAUT.

4. Visão Geral do GT-LFI: o Módulo *Learn-LFI* e sua *Gamified Learning Platform*

O módulo *Learn-LFI* está inserido em um ecossistema de aplicações (GT-LFI) voltado ao aprendizado a partir de incidentes reais de cibersegurança, tendo como propósito central oferecer uma experiência de ensino-aprendizagem gamificada, tornando o processo formativo mais engajante, progressivo e contextualizado com a realidade operacional dos times de segurança. O módulo integra esse ecossistema com o objetivo de transformar incidentes reais, provenientes de parceiros institucionais e devidamente anonimizados pelos módulos anteriores, em conteúdo pedagógico que conecta teoria e prática de maneira dinâmica e acessível. Na Figura 1, é possível visualizar como a GLP do módulo reúne dados reais anonimizados, *feedbacks* de especialistas, tutoriais e recomendações de solução, compondo uma experiência integrada de educação em cibersegurança.

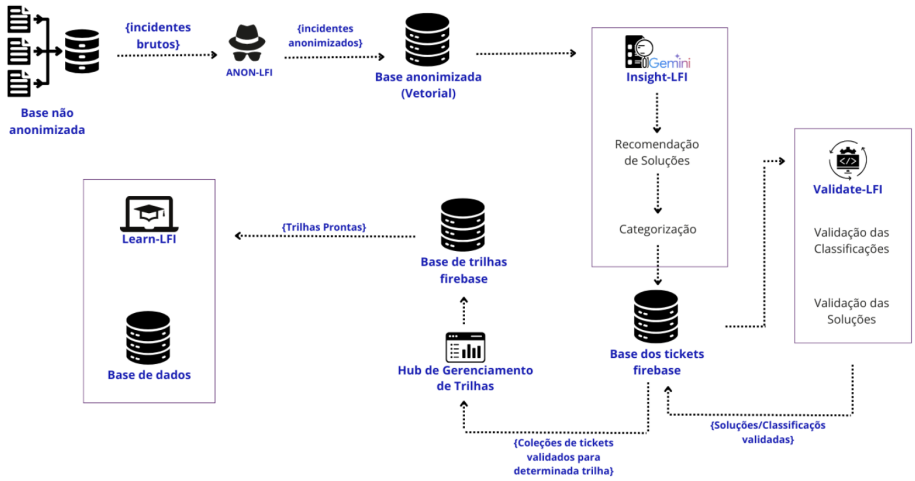


Figura 1. Visão geral da arquitetura da LFI.

O público alvo prioritário do módulo *Learn-LFI* são estudantes do programa de residência tecnológica Hackers do Bem da RNP, geralmente recém graduados ou em transição de carreira, que necessitam de formação aplicada. O domínio dessa área exige

não apenas conceitos técnicos, mas também tomada de decisão sob pressão e raciocínio analítico, que são competências difíceis de desenvolver por meios puramente expositivos. A GLP foi projetada para motivar o usuário por meio da gamificação, oferecendo trilhas progressivas que partem dos fundamentos até cenários avançados de análise e tratamento de ameaças.

A GLP estrutura a experiência do usuário em torno de elementos que estimulam a motivação e a progressão contínua. Pontos ganhos por desafios concluídos funcionam como reforço positivo, níveis e desbloqueio gradual de conteúdo constroem uma curva de aprendizagem controlada, *badges* marcam marcos na jornada formativa, o *leaderboard* estimula a competição saudável entre pares, enquanto *quizzes* e desafios por código promovem a aplicação prática em cenários próximos da realidade operacional. O *feedback* imediato permite aprendizagem corretiva em tempo real, e a loja virtual (onde o usuário adquire avatares e personalizações com os pontos acumulados) cria senso de pertencimento e investimento pessoal na jornada. A plataforma gamificada do GT-LFI está disponível publicamente no repositório de código aberto: `https://github.com/gt-rnp-lfi/hackers-do-bem`. A Tabela 2 apresenta os elementos da GLP.

Tabela 2. Elementos de gamificação da plataforma LFI.

Elemento	Descrição	Objetivo Pedagógico
Pontos (XP)	Ganhos por conclusão de desafios	Reforço positivo e progressão
Badges	Emblemas por marcos alcançados	Reconhecimento e realização
Leaderboard	Classificação entre usuários	Competição saudável
Níveis	Desbloqueio gradual de conteúdo	Curva de aprendizagem
Desafios	CTFs e exercícios de código	Aplicação prática
Feedback	Retorno imediato sobre acertos/erros	Aprendizagem corretiva
Loja Virtual	Avatares e capas adquiridos com XP	Retenção e identidade

A GLP possui quatro trilhas de conhecimento com progressão deliberada, indo do básico ao intermediário. A **Trilha 1: "O que são Incidentes de Segurança?"** estabelece as bases conceituais para que o residente compreenda o universo de ameaças e respostas. A **Trilha 2: "Classificar Incidentes de Segurança"** avança para a capacidade analítica, treinando o residente a categorizar e priorizar eventos de segurança com base em critérios técnicos e metodológicos alinhados às práticas de CSIRTs. A **Trilha 3: "Atividades sobre Incidentes de Segurança: Ataques DDoS com Exemplos em Python"** introduz um nível intermediário de profundidade técnica, integrando teoria, análise de casos reais e implementação prática em linguagem de programação. E, por último, a **Trilha 4: "Playbooks DDoS"**, que são roteiros estruturados baseados em cenários reais que guiam o usuário nas etapas de identificação, resposta e mitigação de ataques de negação de serviço distribuído. A Tabela 3 apresenta o sequenciamento das atividades das trilhas.

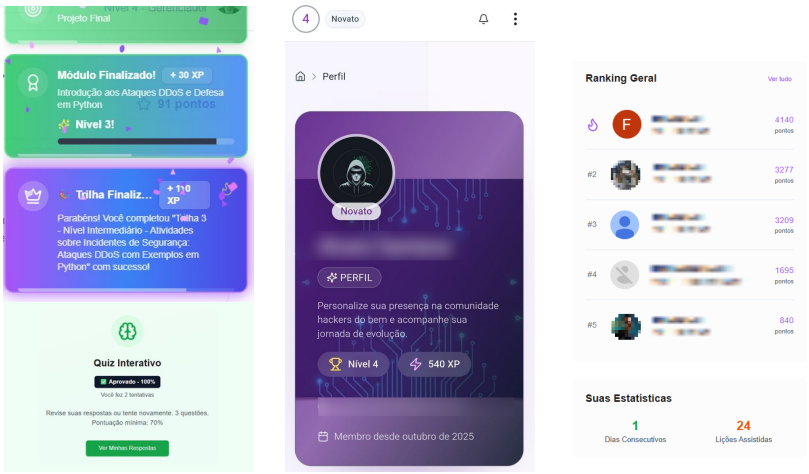
O sequenciamento entre as trilhas segue uma lógica pedagógica, onde cada trilha pressupõe e aprofunda os conhecimentos construídos na anterior, garantindo que a progressão do aprendiz seja sustentada por uma base consolidada antes de avançar para conteúdos mais complexos. Essa arquitetura curricular (básico, intermediário e avançado) reflete uma preocupação com a construção gradual de competências, evitando comprometer a aplicação prática do conhecimento. A GLP também possui suporte ao instrutor para criação de novas trilhas, incluindo algoritmos de inteligência artificial, que auxiliam na

Tabela 3. Estrutura das trilhas de aprendizagem da GLP.

Trilha	Nível	Atividades
T1	Básico	Leitura: evento, alerta e incidente → Quiz: identificação de incidentes → Leitura: tipos comuns de incidentes → Leitura: simulação de impacto de *phishing*
T2	Básico	Leitura: critérios e categorias NIST → Prática: incidentes anonimizados → Quiz: classificação por categoria NIST → Leitura: registro e documentação → Quiz: priorização e comunicação (NIST SP 800-61r3)
T3	Intermediário	Quiz: conceitos DDoS → Quiz: impactos DDoS → Prática: incidentes anonimizados → Quiz: verdadeiro ou falso → Leitura: diagrama de ataque → Projeto prático final
T4	Intermediário	Leitura: introdução a playbooks → Leitura: componentes do playbook → Quiz: componentes do playbook → Leitura: classificação de ataque DDoS → Leitura: fluxo de decisão para resposta → Prática: ações automatizadas de mitigação → Leitura: adaptação de playbooks

criação e personalização de trilhas utilizando incidentes reais anonimizados, adaptando o sequenciamento para atender ao perfil e ao ritmo de evolução do público-alvo.

Para apoiar o residente ao longo desse percurso, a GLP disponibiliza um sistema estruturado de dicas e tutoriais integrados às lições. Esse suporte contextual, presente nos desafios de código, nos *quizzes* e nos exercícios práticos, auxilia o aprendiz a avançar diante de obstáculos e estimula a evolução de maneira orientada, fortalecendo a autonomia e a confiança técnica ao longo da formação.



(a) Quizz **(b)** Perfil **(c)** Ranking

Figura 2. Capturas de telas da GLP.

5. Metodologia

A metodologia deste estudo foi estruturada em duas grandes etapas: *(i)* coleta de dados, que compreendeu o recrutamento, convite, apresentação, utilização da GLP e o preenchimento de um questionário online estruturado, e *(ii)* análise de dados, que adotou uma abordagem mista quali-quantitativa, onde foi aplicado o modelo UTAUT com modelagem PLS-SEM (*Partial Least Squares Structural Equation Modeling*), análise de sentimentos com o léxico OplexiconV3.0 e análise temática dos *feedbacks* recebidos. Ambas as etapas são apresentadas nas subseções a seguir.

5.1. Coleta de Dados

A coleta de dados foi conduzida entre 14 e 26 de janeiro de 2026. Os participantes foram recrutados por convite formal entre os residentes ativos do programa Hackers

do Bem da RNP, configurando uma amostra por conveniência. O convite foi acompanhado de informações detalhadas sobre os objetivos da pesquisa e os procedimentos de participação, seguido do aceite formal do Termo de Consentimento Livre e Esclarecido (TCLE), disponibilizado em formato digital. Após o aceite, foi realizada uma apresentação introdutória do módulo *Learn-LFI* e sua GLP por videoconferência, com o objetivo de nivelar o entendimento sobre as funcionalidades da plataforma e minimizar possíveis vieses decorrentes de dificuldades de navegação. Em seguida, os participantes acessaram a GLP por sete dias, percorrendo quatro trilhas de conhecimento organizadas nos níveis básico e intermediário, cobrindo desde conceitos fundamentais de incidentes de segurança até a análise e mitigação de ataques DDoS com exemplos em Python. Durante esse período, os participantes interagiram livremente com os elementos gamificados da plataforma. Ao término, foram direcionados ao preenchimento de um questionário online estruturado[1], encerrando o ciclo de coleta.

O questionário UTAUT aplicado foi estruturado em seis constructos, cada um composto por itens que mensuram uma dimensão específica da aceitação tecnológica, conforme apresentado na Tabela 4. Cada item representa uma afirmação avaliada em uma escala Likert de 5 pontos (1 = Discordo Totalmente a 5 = Concordo Totalmente), e o conjunto de itens de um mesmo constructo, quando analisado de forma integrada, expressa a percepção do participante sobre essa dimensão. Complementarmente, foram incluídas quatro questões abertas para aprofundar a compreensão qualitativa da experiência dos participantes com a GLP: (1) *"Resuma sua experiência na plataforma"*; (2) *"Qual foi a parte mais difícil ao usar a plataforma pela primeira vez? O que poderia ter tornado esse processo mais fácil?"*; (3) *"O que a plataforma não oferece hoje que seria essencial para melhorar sua experiência?"*; e (4) *"Houve algum desafio ou missão que você achou desnecessário ou irrelevante?"*. Os dados foram obtidos a partir de duas fontes complementares: o questionário estruturado baseado no modelo UTAUT com as questões abertas coletadas, combinado com *feedbacks* recebidos por e-mail sobre a GLP.

5.2. Análise de Dados

A análise dos dados coletados combinou procedimentos quantitativos e qualitativos de forma sequencial: os dados quantitativos foram analisados em primeira instância e, posteriormente, os resultados qualitativos aprofundaram e contextualizaram os achados numéricos. A análise quantitativa foi conduzida em cinco etapas. Primeiro, levantaram-se dados demográficos dos participantes quanto a sexo, faixa etária e experiência prévia com gestão de *tickets* de segurança. Segundo, calcularam-se estatísticas descritivas (médias, desvio padrão, assimetria e curtose) para todos os itens da escala UTAUT, permitindo verificar a distribuição das respostas e identificar eventuais efeitos de teto ou de piso. Terceiro, avaliaram-se as propriedades psicométricas dos constructos por meio do Alfa de Cronbach (α), Confiabilidade Composta (ρ_c) e Variância Média Extraída (AVE), adotando limiares de 0,70 e 0,50. Quarto, aplicamos o PLS-SEM para estimar os coeficientes de caminho (β) entre os constructos preditores (PE, EE, SI, FC e PR) e a Intenção Comportamental (BI), avaliando o ajuste do modelo pelos coeficientes R^2 e R^2_{adj}. Por fim, analisou-se o desempenho dos participantes nos *quizzes* de cada trilha da GLP por meio de *scores* médios e taxas de aprovação, permitindo identificar padrões de assimilação de conteúdo entre as trilhas e sinalizar eventuais necessidades de revisão instrucional.

[1] https://forms.gle/SMKDmvXAK9kweHYu7

Tabela 4. Itens do questionário UTAUT aplicado à GLP.

Item	Constructo	Enunciado
PE1	Expectativa de Desempenho (PE)	Usar a plataforma me ajuda a alcançar meus objetivos de aprendizado rapidamente.
PE2		Usar a plataforma aumenta minha efetividade para alcançar meus objetivos de aprendizado.
PE3		Usar a plataforma melhora minha motivação para alcançar meus objetivos de aprendizado.
PE4		Considero a plataforma útil para melhorar minhas habilidades e alcançar meus objetivos.
PE5		Considero a plataforma útil para minhas necessidades futuras de aprendizado.
EE1	Expectativa de Esforço (EE)	No geral, acredito que a plataforma é fácil de usar.
EE2		Usar a plataforma para aprender demanda pouco tempo.
EE3		Considero fácil interagir com a plataforma.
EE4		Aprender a usar a plataforma é fácil para mim.
EE5		Minhas atividades de aprendizado na plataforma são claras e compreensíveis.
EE6		Considero fácil alcançar meus objetivos de aprendizado com a plataforma.
SI1	Influência Social (SI)	Pessoas importantes para mim acham que eu deveria usar a plataforma para aprender.
SI2		Pessoas influentes usam a plataforma para aprender.
SI3		Conheço outras pessoas que usam a plataforma para aprender.
SI4		Acho a plataforma uma ferramenta de ensino atual.
FC1	Condições Facilitadoras (FC)	Tenho os recursos necessários para usar a plataforma.
FC2		Tenho o conhecimento necessário para usar a plataforma.
FC3		Usar a plataforma combina bem com a forma como gosto de aprender.
FC4		Tenho acesso fácil e regular à internet para usar a plataforma.
FC5		Tenho um ambiente conveniente para usar a plataforma.
FC6		Se tiver problemas usando a plataforma, consigo resolvê-los rapidamente.
PR1	Risco Percebido (PR)	Sinto que minhas preocupações com confidencialidade são atendidas ao usar a plataforma.
PR2		Acredito que minha privacidade está adequadamente protegida ao usar a plataforma.
PR3		Confio na plataforma como ferramenta de aprendizado.
PR4		Prefiro a plataforma a um instrutor humano.
PR5		Acredito que não tenho riscos ao usar a plataforma.
BI1	Intenção Comportamental (BI)	Pretendo usar a plataforma em minhas futuras atividades de aprendizado.
BI2		Prevejo que usarei a plataforma para aprender.
BI3		Planejo usar a plataforma nos próximos 2 meses.
BI4		Recomendaria a plataforma a um amigo.

A análise qualitativa foi conduzida em duas partes complementares: *(i)* análise de sentimentos das respostas abertas com base no léxico OplexiconV3.0, léxico para o português brasileiro com polaridade semântica positiva $(+1)$, negativa (-1) ou neutra (0), considerando valores positivos como percepção favorável ao item avaliado, negativos indicando rejeição ao item avaliado e próximos de zero indicando neutralidade sobre o item avaliado; e *(ii)* análise temática de e-mails recebidos como *feedback*, por meio da qual as menções foram codificadas e categorizadas em cinco categorias: *bugs*, usabilidade, material didático, estrutura de ensino e funcionalidade. Para cada categoria, foram contabilizadas separadamente as menções críticas e as menções positivas, permitindo uma síntese sistemática dos pontos de atrito e das forças percebidas na plataforma. A triangulação entre os resultados quantitativos e qualitativos foi conduzida de forma paralela, comparando os achados para identificar convergências, divergências e complementaridades.

6. Resultados e Discussões

Os resultados obtidos a partir da avaliação da GLP são apresentados a seguir, organizados em cinco subseções: perfil dos participantes, estatísticas descritivas da escala UTAUT, confiabilidade e validade dos constructos, análise qualitativa, modelagem PLS-SEM e desempenho dos usuários nas trilhas.

6.1. Perfil dos Participantes

Conforme apresentado na Tabela 5, houve predominância do sexo masculino (80,0%, n=28) e de participantes com idade superior a 30 anos (83,0%, n=29). Em relação à experiência prévia com gestão de *tickets*, observou-se uma distribuição heterogênea: 28,6% dos participantes declararam não possuir nenhuma experiência, enquanto 14,3% relataram mais de um ano de experiência, sinalizando uma amostra com perfis técnicos variados.

Tabela 5. Perfil demográfico dos participantes.

Variável	Categoria	N	%
Sexo	Masculino	28	80,0
	Feminino	7	20,0
Faixa etária	20–25 anos	3	8,5
	25–30 anos	3	8,5
	>30 anos	29	83,0
Exp. prévia c/ tickets	Sem experiência	10	28,6
	Até 3 meses	7	20,0
	3–6 meses	6	17,1
	6 m. a 1 ano	7	20,0
	>1 ano	5	14,3

6.2. Análise da Aceitação e Intenção de Uso - Escala UTAUT

Como mostra a Tabela 6, que inclui as médias, desvios padrão (DP), assimetria (Ass.) e curtose (Cur.) dos itens da escala *Likert* (1–5), as avaliações foram predominantemente positivas nos constructos PE (médias entre 4,23 e 4,54), EE (3,97 a 4,77) e BI (4,06 a 4,63), com desvios padrão reduzidos, indicando percepção consistente entre os participantes. O item EE4 obteve a maior média da escala (M = 4,77; DP = 0,43), e BI4 registrou a maior média do constructo de Intenção Comportamental (M = 4,63; DP = 0,69), refletindo forte intenção de adoção da GLP. O constructo SI apresentou maior variabilidade (médias entre 3,00 e 4,20), sugerindo percepções heterogêneas quanto ao entorno social. Os itens de Risco Percebido (PR) registraram médias baixas (entre 1,43 e 3,23), indicando baixa percepção de risco associada ao uso da GLP. As Condições Facilitadoras (FC) apresentaram as maiores médias da escala, com FC4 e FC5 atingindo M = 4,94 (DP = 0,24); contudo, os elevados valores de curtose e assimetria negativa apontam para efeito de teto nesses itens, limitando sua variabilidade para análises mais aprofundadas.

A Tabela 7 apresenta os índices de confiabilidade e validade convergente dos constructos. PE, EE, SI, PR e BI atenderam aos critérios mínimos estabelecidos (α e $\rho_c >$ 0,70; AVE $>$ 0,50), com destaque para BI, que apresentou desempenho excelente (α = 0,907; AVE = 0,785). O constructo FC foi reprovado em todos os critérios (AVE = 0,285; ρ_c = 0,370), com cargas fatoriais negativas nos itens FC2, FC4 e FC5. O modelo explicou 48,4% da variância da Intenção Comportamental (BI), com R^2_{adj} = 0,395. A Expectativa de Esforço (EE) foi o preditor de maior efeito positivo (β = 0,325), seguida pela Influência Social (β = 0,204) e pelas Condições Facilitadoras (β = 0,131). O Risco Percebido apresentou efeito negativo esperado (β = $-$0,283), coerente com o pressuposto de que uma menor percepção de risco favorece a intenção de uso. A Expectativa de Desempenho registrou coeficiente negativo (β = $-$0,149), que apresentou um resultado contraintuitivo.

Tabela 6. Estatísticas descritivas dos itens da escala UTAUT.

Item	Constructo	Média	DP	Ass.	Cur.	Item	Constructo	Média	DP	Ass.	Cur.
PE1		4,29	0,62	−0,25	−0,76	**PR1**		1,71	0,83	0,54	−1,36
PE2		4,43	0,61	−0,50	−0,77	**PR2**		1,69	0,87	0,89	−0,42
PE3	Expectativa de Desempenho	4,29	0,75	−0,49	−1,14	**PR3**	Risco Percebido	1,43	0,81	1,65	1,50
PE4		4,54	0,56	−0,65	−0,76	**PR4**		3,23	1,19	−0,13	−1,21
PE5		4,23	0,77	−0,39	−1,27	**PR5**		2,20	1,11	0,63	−0,54
EE1		4,51	0,66	−0,95	−0,31	**FC1**		4,80	0,58	−3,41	12,50
EE2		4,09	0,89	−0,41	−1,10	**FC2**		4,74	0,51	−1,70	2,02
EE3	Expectativa de Esforço	4,46	0,70	−0,85	−0,60	**FC3**	Condições Facilitadoras	4,20	0,83	−0,66	−0,51
EE4		4,77	0,43	−1,24	−0,48	**FC4**		4,94	0,24	−3,65	11,68
EE5		4,14	0,85	−0,83	0,14	**FC5**		4,94	0,24	−3,65	11,68
EE6		3,97	0,98	−1,02	0,80	**FC6**		4,06	0,87	−0,62	−0,40
SI1		3,26	1,01	−0,01	−0,05	**BI1**		4,37	0,84	−1,04	−0,03
SI2	Influência Social	3,00	0,91	0,23	0,71	**BI2**	Intenção Comportamental	4,43	0,81	−1,20	0,50
SI3		3,60	1,42	−0,44	−1,15	**BI3**		4,06	1,08	−1,19	1,05
SI4		4,20	0,90	−0,85	−0,23	**BI4**		4,63	0,69	−2,02	4,14

DP = Desvio Padrão; Ass. = Assimetria; Cur. = Curtose.

Tabela 7. Confiabilidade e validade convergente dos constructos (PLS-SEM).

Constructo	α	ρ**A**	ρ**c**	**AVE**	**Status**
PE — Expect. Desempenho	0,886	0,957	0,912	0,675	Aprovado
EE — Expect. Esforço	0,823	0,880	0,868	0,534	Aprovado
SI — Influência Social	0,727	0,838	0,816	0,529	Aprovado
FC — Cond. Facilitadoras	0,703	1,150	0,370	0,285	**Reprovado**
PR — Risco Percebido	0,765	0,760	0,838	0,511	Aprovado
BI — Intenção Comport.	0,907	0,909	0,936	0,785	Excelente

Critérios: α e ρc $> 0{,}70$; AVE $> 0{,}50$. FC falha em todos os critérios.

6.3. Análise Qualitativa

A análise de sentimentos das respostas abertas resultou em um score médio positivo de 0,51 para a percepção geral da GLP. As dimensões "dificuldades encontradas na GLP", "o que falta de essencial na GLP" e "itens desnecessários da GLP" obtiveram scores neutros, sinalizando que as críticas não foram acompanhadas de rejeição à proposta da plataforma. A análise temática dos *feedbacks*, sintetizados na Tabela 8, identificou 47 menções críticas e 32 positivas, distribuídas em cinco categorias. *Bugs* concentraram o maior volume de críticas (18 menções), seguidos por problemas de usabilidade (15 críticas; 5 elogios). Em contraste, o material didático (15 elogios; 8 críticas) e a estrutura de ensino (10 elogios; 6 críticas) foram os principais pontos fortes percebidos pelos participantes.

Tabela 8. Feedbacks qualitativos por categoria temática.

Categoria	**Ajustes/Críticas**	**Pontos positivos**
Bugs	18	—
Usabilidade	15	5
Material didático	8	15
Estrutura de ensino	6	10
Funcionalidade	—	2
Total	**47**	**32**

6.4. Trilhas

A Tabela 9 apresenta os resultados de desempenho por trilha. As Trilhas 1, 3 e 4 obtiveram altas taxas de aprovação, com destaque para a Trilha 3 - Ataques DDoS com Python, que registrou o melhor desempenho geral (score médio = 93,1; aprovação = 84,3%). A Trilha 2 configurou o principal ponto de atrito da jornada com 94 tentativas, o maior volume entre todas as trilhas, registrou o menor score médio (65,3) e a menor taxa de aprovação (54,3%) da GLP.

Tabela 9. Desempenho por trilha nos quizzes.

Trilha	Tent.	Score méd.	Aprovação	Status
T1 — Incidentes (intro)	36	77,5	80,6%	Ok
T2 — Classificar incidentes	94	65,3	54,3%	**Crítico**
T3 — Ataques DDoS c/ Python	70	93,1	84,3%	Ok
T4 — Playbooks DDoS	35	83,8	82,9%	Ok

7. Discussões e implicações

Os resultados indicam boa recepção da GLP em sua versão inicial. As médias acima de 4,0 (PE, EE e BI) sugerem que a plataforma foi percebida como útil, fácil de usar e com forte potencial de adoção. A análise qualitativa reforça esse resultado, com escore positivo de 0,51 e destaque para o material didático e a estrutura de ensino. O desempenho nas trilhas corrobora essa percepção: três das quatro trilhas atingiram taxas de aprovação superiores a 80,0%, sendo a exceção a Trilha 2 (54,3%), que sinaliza necessidade de revisão instrucional e ajuste na progressão dos desafios. *Bugs* e problemas de usabilidade concentraram as principais críticas, resultado esperado em soluções em estágio inicial.

O modelo PLS-SEM revelou a EE como principal preditor da intenção de uso (β = 0,325), seguida pela Influência Social (β = 0,204), indicando que a facilidade de uso e o reconhecimento social são determinantes na adoção da plataforma. Em contextos de treinamento técnico, nos quais os conteúdos já apresentam elevada complexidade cognitiva, reduzir barreiras operacionais pode contribuir diretamente para a permanência e o engajamento dos usuários. Complementarmente, o efeito positivo da Influência Social sugere que fatores externos, como recomendações de colegas, instrutores ou comunidades técnicas, também exercem um papel relevante na aceitação da plataforma.

Por outro lado, o coeficiente negativo associado à PE apresentou um resultado contraintuitivo. Uma possível interpretação é que participantes com expectativas mais elevadas em relação aos benefícios práticos da plataforma tenham adotado uma postura mais crítica durante a avaliação, especialmente diante de limitações técnicas identificadas nos *feedbacks* qualitativos, como *bugs* e problemas de usabilidade. Esse resultado também pode refletir a natureza exploratória da amostra e o fato de a GLP ainda se encontrar em estágio inicial de consolidação. O efeito negativo do Risco Percebido ($\beta = -0{,}283$) é teoricamente coerente e reforça a confiança dos participantes, favorecendo a adoção de tecnologias digitais. O constructo FC foi reprovado em todos os critérios do PLS-SEM, possivelmente pelo efeito de teto decorrente do acesso uniforme à infraestrutura por todos os participantes, indicando a necessidade de revisão de seus itens em ciclos futuros.

A análise qualitativa complementa os resultados quantitativos ao demonstrar que, embora os participantes tenham percebido valor pedagógico na plataforma, persistem de-

safios relacionados à estabilidade e à experiência de uso. As críticas associadas a *bugs* e usabilidade evidencia que problemas técnicos podem comprometer a experiência de aprendizagem, mesmo em contextos nos quais há percepção positiva sobre o conteúdo ofertado. Como limitações, aponta-se principalmente o tamanho amostral, que restringe o poder estatístico e impede generalizações, tornando a ampliação da amostra condição necessária para explorar plenamente o potencial preditivo do modelo. Além disso, o perfil dos respondentes caracteriza-se por uma amostra restrita.

8. Conclusão

Este trabalho teve como objetivo avaliar a motivação e a intenção de uso de uma GLP voltada à educação em tratamento e resposta a incidentes, investigando em que medida seus elementos de gamificação influenciam o engajamento dos usuários. Para isso, adotou-se uma abordagem quali-quantitativa: o modelo UTAUT, operacionalizado por meio de PLS-SEM, foi utilizado para mensurar a aceitação tecnológica, enquanto os *feedbacks* e as respostas às questões abertas permitiram aprofundar a compreensão dos fatores subjetivos associados à adesão.

Os resultados obtidos indicam que a plataforma demonstrou potencial de adoção entre os participantes, com a Expectativa de Esforço e a Influência Social como fatores de maior peso preditivo sobre a intenção de uso. O modelo PLS-SEM explicou aproximadamente metade da variância da intenção de uso ($R^2 = 0{,}484$), resultado expressivo para uma primeira rodada avaliativa com amostra reduzida. Os dados qualitativos corroboraram e complementaram esses achados, sinalizando *bugs* na interface e aspectos motivacionais não plenamente capturados pelas métricas quantitativas.

Para trabalhos futuros, pretende-se incorporar os ajustes identificados no sistema, ampliar o tamanho amostral, aprimorar o instrumento de coleta e conduzir uma comparação da intenção de uso entre versões da plataforma com e sem gamificação, de modo a isolar o efeito específico dos elementos gamificados sobre o engajamento e a adoção pelos usuários.

Agradecimentos

O presente trabalho foi realizado com o apoio do 'Programa Hackers do Bem no Domínio Cibernético', executado pela RNP e SENAI, coordenado pela Softex e financiado pelo MCTI com recursos oriundos da Lei das TICs - Lei nº 8.248, de 23 de outubro de 1991. Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) projetos 409743/2025-9 e 408432/2024-1. Agradecemos ao Programa de Pós-Graduação em Ciência da Computação (PPGCO/FACOM/UFU) pelo suporte a pesquisa.

Declaração sobre o uso de Inteligência Artificial

Os autores declaram o uso de modelos de linguagem de grande porte (LLMs), como ChatGPT e Claude, exclusivamente como ferramentas de apoio à fluidez e aprimoramento da redação de parágrafos deste artigo. Todas as ideias, interpretações, análises e conclusões apresentadas são de responsabilidade integral dos autores.

Referências

[Al-Momani and Ramayah 2025] Al-Momani, A. and Ramayah, T. (2025). The utaut model in understanding ehr adoption: a systematic review. *Intelligence-Driven Circular Economy: Regeneration Towards Sustainability and Social Responsibility—Volume 2*, pages 179–194.

[Almaiah et al. 2019] Almaiah, M. A., Alamri, M. M., and Al-Rahmi, W. (2019). Applying the UTAUT model to explain the students' acceptance of mobile learning system in higher education. *IEEE Access*, 7:174673–174686.

[Ashley et al. 2022] Ashley, T. D., Kwon, R., Gourisetti, S. N. G., Katsis, C., Bonebrake, C. A., and Boyd, P. A. (2022). Gamification of cybersecurity for workforce development in critical infrastructure. *Ieee Access*, 10:112487–112501.

[Attuquayefio and Addo 2014] Attuquayefio, S. and Addo, H. (2014). Review of studies with utaut as conceptual framework. *European scientific journal*, 10(8).

[Bayır and Akel 2024] Bayır, T. and Akel, G. (2024). Gamification in mobile shopping applications: A review in terms of technology acceptance model. *Multimedia Tools and Applications*, 83(16):47247–47268.

[Busarello 2016] Busarello, R. I. (2016). *Gamification: princípios e estratégias*. Pimenta Cultural, São Paulo.

[Cybrary 2026] Cybrary (2026). Cybrary: Cybersecurity professional development platform. Disponível em: `https://www.cybrary.it/`. Acesso em: 03 mai. 2026.

[ENAP 2026] ENAP (2026). Ev.g. - escola virtual gov. Disponível em: `https://www.escolavirtual.gov.br/`. Acesso em: 03 mai. 2026.

[Google 2026a] Google (2026a). Interland — be internet awesome. Disponível em: `https://beinternetawesome.withgoogle.com/pt-br_br/interland`. Acesso em: 03 mai. 2026.

[Google 2026b] Google (2026b). Space shelter: Jogo de segurança online. Disponível em: `https://spaceshelter.withgoogle.com/intl/pt_pt/`. Acesso em: 03 mai. 2026.

[GT-LFI – Learning From Incidents 2026] GT-LFI – Learning From Incidents (2026). Gt-lfi: Inovação em cibersegurança. Disponível em: `https://gt-rnp-lfi.github.io/home/`. Acessado em: 02 ago. 2026.

[HackTheBox 2026] HackTheBox (2026). Hackthebox. Disponível em: `https://www.hackthebox.com/`. Acesso em: 03 mai. 2026.

[Hair et al. 2021] Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., and Ray, S. (2021). *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*. Classroom Companion: Business. Springer.

[IBSEC 2026] IBSEC (2026). Instituto brasileiro de cibersegurança. Disponível em: `https://ibsec.com.br/`. Acesso em: 03 mai. 2026.

[ISC2 2024] ISC2 (2024). Cybersecurity workforce 2024. `https://www.isc2.org/Insights/2024/10/Cybersecurity-Workforce-INSIGHTS-October-2024`. Acesso em: maio de 2026.

[Karagiannis and Magkos 2021] Karagiannis, S. and Magkos, E. (2021). Adapting ctf challenges into virtual cybersecurity learning environments. *Information & Computer Security*, 29(1):105–132.

[KC7 Cyber 2026] KC7 Cyber (2026). Kc7: Cybersecurity learning platform. Disponível em: `https://kc7cyber.com/`. Acesso em: 03 mai. 2026.

[Khoo and Johnkhan 2017] Khoo, C. S. G. and Johnkhan, S. B. (2017). Lexicon-based sentiment analysis: Comparative evaluation of six sentiment lexicons. *Journal of Information Science*, pages 1–21.

[Khoo and Johnkhan 2018] Khoo, C. S. G. and Johnkhan, S. B. (2018). Lexicon-based sentiment analysis: Comparative evaluation of six sentiment lexicons. *Journal of Information Science*, 44(4):491–511.

[Lopes et al. 2024] Lopes, W., Augusto, P., Fernandes, I., and Madeira, C. (2024). Proposal for a gamification strategy applied to remote learning. *Journal on Interactive Systems*, 15(1):92–103.

[Mostafa and Faragallah 2019] Mostafa, M. and Faragallah, O. S. (2019). Development of serious games for teaching information security courses. *IEEE Access*, 7:169293–169305.

[Olaniyi 2025] Olaniyi, O. M. (2025). A quantitative approach to understanding machine learning adoption for cybersecurity in e-commerce through the utaut model. *Journal of Engineering Research and Reports*, 27(11):286–304.

[Organização das Nações Unidas 2015] Organização das Nações Unidas (2015). Objetivo de desenvolvimento sustentável 4: Educação de qualidade. `https://brasil.un.org/pt-br/sdgs/4`. Acesso em: 17 maio 2026.

[OverTheWire 2026] OverTheWire (2026). Bandit — overthewire wargames. Disponível em: `https://overthewire.org/wargames/bandit/`. Acesso em: 03 mai. 2026.

[Pirta-Dreimane et al. 2024] Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., and Bonders, M. (2024). Try to escape from cybersecurity incidents! a technology-enhanced educational approach. *Technology, Knowledge and Learning*, pages 1–30.

[SBC 2023] SBC (2023). *Referenciais de Formação para o Curso de Bacharelado em CiberSegurança*. Sociedade Brasileira de Computação, Porto Alegre.

[Shahzadi et al. 2025] Shahzadi, A., Ishaq, K., Nawaz, N. A., Rosdi, F., and Khan, F. A. (2025). Unveiling personalized and gamification-based cybersecurity risks within financial institutions. *PeerJ Computer Science*, 11:e2598.

[Sociedade Brasileira de Computação 2025] Sociedade Brasileira de Computação (2025). *Grandes Desafios da Computação no Brasil 2025-2035*. Sociedade Brasileira de Computação (SBC), Porto Alegre, RS, Brasil. Acesso em: 17 maio 2026.

[Sodikin and Hikmawan 2023] Sodikin, R. A. and Hikmawan, R. (2023). Analysis of gamification in cybersecurity education for students: A systematic literature review. *Jurnal Educative: Journal of Educational Studies*, 8(2):147–166.

[Thombre and Velankar 2022] Thombre, S. and Velankar, M. (2022). Gamification by students: An effective approach to cyber security concept learning. *Journal of Engineering Education Transformations*, pages 73–81.

[TryHackMe 2026] TryHackMe (2026). Tryhackme: Cybersecurity training platform. Disponível em: `https://tryhackme.com/`. Acesso em: 03 mai. 2026.

[Venkatesh et al. 2003] Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3):425–478.

[Zorzo et al. 2017] Zorzo, A. F., Nunes, D., Matos, E. S., Steinmacher, I., Leite, J. C., Araujo, R. M., Correia, R. C. M., and Martins, S. (2017). *Referenciais de Formação para os Cursos de Graduação em Computação*. Sociedade Brasileira de Computação.