



Gamificação no ensino de cibersegurança: desenvolvimento de um aplicativo educacional interativo

Antonio Roberto Cursino Filho | antonio.rcf16@aluno.ifsc.edu.br¹
Isadora Reginatto Pompermaier | isadora.p02@aluno.ifsc.edu.br²
Letycia Araldi | letycia.a12@aluno.ifsc.edu.br³
João Vitor Bosetti | joao.b2009@aluno.ifsc.edu.br⁴
Ketllyn Tomkelski de Andrade | ketllyn.a@aluno.ifsc.edu.br⁵
Ynaiê Chiarello | lynaie.c@aluno.ifsc.edu.br⁶
Michel Kramer Borges de Macedo | michel.kramer@ifsc.edu.br⁷

Trabalho de Ensino e Pesquisa
DT 3 - Educação, Cidadania, Desenvolvimento Social e Práticas Inclusivas

Resumo:

O trabalho aborda a necessidade de ampliar o conhecimento sobre cibersegurança diante do aumento das ameaças digitais e das lacunas na formação de estudantes da área de tecnologia. O objetivo é desenvolver um aplicativo educacional gamificado para apoiar a aprendizagem de conceitos básicos de segurança digital. A metodologia envolve revisão bibliográfica, levantamento de requisitos, desenvolvimento iterativo do protótipo e avaliação com estudantes por meio de testes e questionários. A solução proposta inclui desafios interativos, simulações e mecanismos de gamificação para estimular o engajamento e a aprendizagem ativa. Como contribuição, espera-se gerar uma ferramenta tecnológica de apoio ao ensino, além de produzir conhecimento sobre o uso da gamificação na educação em cibersegurança, contribuindo para práticas pedagógicas mais inovadoras e eficazes.

Palavras-chave: gamificação; cibersegurança; tecnologias educacionais; aprendizagem interativa.

Introdução

Nas últimas décadas, o avanço das tecnologias digitais transformou a forma como as pessoas se comunicam, trabalham, estudam e acessam informações, ampliando o uso de sistemas computacionais, dispositivos móveis e serviços online. Embora o uso de tecnologias digitais tenha ampliado a conectividade e o acesso à informação, também

¹ Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

² Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

³ Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

⁴ Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

⁵ Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

⁶ Estudante do Curso de Informática do IFSC-Câmpus Xanxerê.

⁷ Professor do Curso de Informática do IFSC-Câmpus Xanxerê.

aumentou a exposição dos usuários a riscos no ambiente virtual. Segundo a Kaspersky (2024), o Brasil registrou quase 2 milhões de ataques de *malware* por dia entre junho de 2023 e julho de 2024, sendo o país mais atacado da América Latina.

De acordo com a Kaspersky (2023), cerca de 40% dos brasileiros não sabem como seus dados são coletados na internet. Essa falta de conhecimento sobre boas práticas de segurança digital aumenta a vulnerabilidade a golpes e fraudes online. O relatório Norton Cyber Safety Insights (2023) aponta ainda que um em cada três brasileiros já foi vítima de golpe ou tentativa de fraude na internet.

Diante desse contexto, a cibersegurança torna-se cada vez mais relevante nos âmbitos sociais, educacionais e profissionais. Entretanto, o ensino de segurança da informação nem sempre é acessível ou envolvente para estudantes em formação na área de tecnologia, pois conteúdos técnicos e abstratos podem dificultar a assimilação prática e reduzir o engajamento no aprendizado. Portanto, a gamificação surge como uma abordagem pedagógica que utiliza elementos de jogos, como desafios, pontuações, níveis e recompensas, para estimular a participação, a motivação e a compreensão de conteúdos complexos por meio de uma aprendizagem mais dinâmica e interativa.

A pesquisa propõe o desenvolvimento de um aplicativo educacional gamificado para o ensino de conceitos básicos de cibersegurança, com desafios e atividades sobre segurança digital, como criação de senhas seguras e proteção de dados. O objetivo é promover a conscientização sobre segurança digital entre estudantes de tecnologia da informação, estruturando conteúdos interativos, utilizando elementos de gamificação para estimular o engajamento e analisando seu potencial como ferramenta de apoio ao ensino.

Ao integrar ensino, pesquisa e desenvolvimento tecnológico, o projeto busca contribuir para a formação de estudantes conscientes para lidar com os desafios da segurança digital na sociedade contemporânea, além de incentivar o uso de metodologias educacionais inovadoras no ensino de tecnologia.

Fundamentação teórica OU Descrição do público envolvido

A cibersegurança envolve práticas, tecnologias e processos destinados à proteção de sistemas, redes e dados contra acessos não autorizados, ataques ou danos, garantindo os princípios de confidencialidade, integridade e disponibilidade das

informações (Whitman; Mattord, 2018). Além das soluções tecnológicas, o fator humano possui papel central, já que muitos incidentes de segurança estão relacionados a comportamentos inadequados dos usuários, como uso de senhas fracas, compartilhamento indevido de dados e dificuldade em reconhecer tentativas de engenharia social.

Além disso, a gamificação surge como uma estratégia pedagógica capaz de aumentar o engajamento e a motivação no processo de aprendizagem. Conforme Deterding *et al.* (2011), a gamificação consiste na aplicação de elementos de jogos em contextos não lúdicos para estimular a participação e promover maior interatividade. No ambiente educacional, essa abordagem favorece a aprendizagem ativa e a compreensão de conteúdos complexos por meio de desafios, *feedback* imediato e progressão de níveis (Kapp, 2012).

A integração entre cibersegurança e gamificação possibilita experiências de aprendizagem mais dinâmicas, permitindo simular situações do ambiente digital e desenvolver habilidades de identificação de riscos. Assim, ferramentas educacionais gamificadas apresentam potencial para apoiar o ensino de segurança da informação de forma mais participativa.

O público-alvo do projeto inclui estudantes e usuários de tecnologias digitais, especialmente aqueles em processo de formação ou que utilizam frequentemente a internet e dispositivos conectados. Ao incentivar a conscientização sobre segurança digital, a proposta busca contribuir para a formação de cidadãos mais preparados para lidar com os riscos do ambiente digital, ampliando seus impactos para além do contexto educacional.

Procedimentos metodológicos

A presente pesquisa caracteriza-se como aplicada, com abordagem qualitativa e quantitativa, envolvendo o desenvolvimento de uma solução tecnológica e sua avaliação em contexto educacional.

Inicialmente foi realizada uma revisão bibliográfica sobre cibersegurança, gamificação e tecnologias educacionais, com o objetivo de fundamentar teoricamente o desenvolvimento do aplicativo e identificar boas práticas relacionadas ao ensino desses

conteúdos. Essa etapa permitirá compreender conceitos essenciais da área e orientar a definição das funcionalidades educacionais da aplicação.

Em seguida foi conduzida a etapa de levantamento de requisitos, na qual foram definidas as principais funcionalidades do sistema, os conteúdos abordados e os elementos de gamificação a serem incorporados, incluindo pontuação, níveis de progressão, *feedback* imediato e desafios interativos.

O desenvolvimento do aplicativo segue uma abordagem iterativa baseada em princípios de metodologias ágeis, inspirada na metodologia Scrum, permitindo ajustes contínuos durante o desenvolvimento. Estão sendo utilizadas tecnologias compatíveis com o desenvolvimento de aplicações *web* ou *mobile*, incluindo *frameworks* de desenvolvimento *front-end* e *back-end*, além de ferramentas de controle e versionamento de código, como o Git.

A aplicação contará com módulos interativos de aprendizagem, incluindo questionários, simulações e desafios práticos relacionados a situações de risco no ambiente digital. Essas atividades buscarão estimular a participação ativa dos usuários e favorecer a compreensão de conceitos relacionados à segurança digital por meio da resolução de problemas e da tomada de decisões em contextos simulados.

Para avaliar a solução proposta, será realizada uma aplicação piloto com estudantes de cursos técnicos integrados ao ensino médio do IFSC Câmpus Xanxerê, que participarão como usuários na fase de testes do aplicativo. A coleta de dados ocorrerá por meio de questionários estruturados e da análise do desempenho dos usuários na plataforma. Eles serão analisados quantitativamente, com cálculo de médias e percentuais relacionados à usabilidade, engajamento e compreensão dos conteúdos. Além disso, serão examinados indicadores de desempenho na plataforma, como taxa de acertos, tempo médio de resolução dos desafios e progressão entre níveis, buscando identificar evidências do impacto do aplicativo no processo de aprendizagem.

O gerenciamento do projeto ocorre por meio da definição de etapas, cronograma e reuniões periódicas de acompanhamento, valorizando o protagonismo dos estudantes envolvidos no processo de desenvolvimento e aprendizagem. Como pontos críticos do projeto, destacam-se a adequação dos elementos de gamificação ao perfil dos estudantes, a usabilidade do aplicativo e a integração entre os conteúdos educacionais e

os mecanismos de interatividade. Esses aspectos serão validados durante a fase de testes com os usuários.

Resultados e discussões

A partir da revisão bibliográfica e da definição dos objetivos, foram estabelecidos os conteúdos do aplicativo educacional, incluindo criação de senhas seguras, identificação de *phishing*, proteção de dados pessoais e comportamentos seguros no ambiente digital, organizados em desafios interativos, questionários e simulações.

Também foram definidos os requisitos funcionais e não funcionais do sistema, prevendo funcionalidades como desafios, questionários, sistema de pontuação, progressão por níveis e *feedback* imediato.

Figura 1 – Requisitos Funcionais e Não Funcionais

ID	Requisitos Funcionais
FR01	O sistema deve permitir cadastro de usuário (dados: nome, apelido, nome de usuário, e-mail e senha)
FR02	O sistema deve permitir que o usuário acesse a opção de esqueceu a senha e ele poderá redefinir-la caso necessário
FR03	O sistema deve exibir uma mensagem de boas-vindas personalizado e depois apresentar um vídeo de introdução
FR04	O sistema deve permitir o usuário importe uma foto de perfil e caso preferir utilizar o user padrão
FR05	O sistema deve apresentar uma aba principal e nela listar as fases/níveis disponíveis e exibir seus nomes, porém bloquear o acesso as ainda não alcançadas
FR06	O sistema deve permitir que o usuário acesse o conteúdo, as questões e os jogos das fases/níveis anteriores e da atual
FR07	O sistema deve apresentar uma aba de conquistas que apresente os objetivos necessários para ganhar as medalhas e mostrar as já obtidas
FR08	O sistema deve calcular e exibir a porcentagem de progresso do jogador para conquistar as medalhas
FR09	O sistema deve desbloquear novas missões a medida que as metas de XP são concluídas
FR10	O sistema deve apresentar uma aba de perfil, que exiba foto, nickname, nível e fase atual, Xp total, conquistas e medalhas obtidas
FR11	O sistema deve permitir editar suas informações de perfil como senha, e-mail e nickname e a opção de exclusão da conta, com o aviso de perda irreversível de dados
FR12	O sistema deve aprovar o usuário para a próxima fase se ele atingir uma pontuação mínima predefinida no jogo final, caso não atingir esta pontuação reinicia-se o jogo
FR13	O sistema deve gerar um certificado de conclusão de curso quando o usuário finalizar o curso e permitir a impressão do mesmo.
ID	Requisitos Não-Funcionais
FR01	As senhas devem ter uma política de complexidade mínima, como 8 caracteres, com a obrigatoriedade de pelo menos uma letra maiúscula, um número e um caractere especial
FR02	A aplicação deve ser responsiva, garantindo que a interface se adapte a diferentes dispositivos e tamanhos de tela dos smartphones.
FR03	O sistema deve fornecer feedback claro e rápido para o usuário sobre ações realizadas (como sucesso ou erro no login, cadastro e recuperação de senha).
FR04	O sistema deve ser compatível com as versões mais recentes dos navegadores mais populares
FR05	O sistema deve solicitar o consentimento explícito do usuário para coletar seus dados pessoais, informando-os sobre a finalidade do uso e o tratamento dos dados.

Fonte: Autoria própria.

A equipe foi organizada com a divisão de responsabilidades entre os estudantes e atualmente, o projeto está na fase de desenvolvimento, com implementação gradual das funcionalidades do aplicativo. A próxima etapa será a realização de testes com estudantes do ensino médio técnico do IFSC Câmpus Xanxerê, para avaliar usabilidade, engajamento e compreensão dos conteúdos.

Espera-se que os resultados obtidos nessa etapa possibilitem analisar o potencial do aplicativo como ferramenta de apoio ao ensino de cibersegurança, contribuindo para a

compreensão de como estratégias baseadas em gamificação podem favorecer processos de aprendizagem mais interativos e participativos no contexto da educação em tecnologia.

Considerações finais

O projeto avançou na criação de uma proposta educacional para o ensino de conceitos básicos de cibersegurança por meio da gamificação. Além disso, contribuiu para a formação acadêmica e profissional dos estudantes ao integrar pesquisa, desenvolvimento tecnológico e metodologias educacionais inovadoras, fortalecendo a relação entre teoria e prática e estimulando competências técnicas e investigativas.

Por fim, o trabalho busca materializar a indissociabilidade entre ensino, pesquisa e extensão, ao propor o desenvolvimento de uma ferramenta educacional que poderá beneficiar estudantes e disseminar conhecimentos sobre segurança digital. Com a continuidade do projeto e a realização de testes e avaliações, espera-se ampliar o impacto da proposta e consolidar o aplicativo como um recurso de apoio ao ensino de cibersegurança em contextos educacionais.

Referências

DETERDING, Sebastian; DIXON, Dan; KHALED, Rilla; NACKE, Lennart. From game design elements to gamefulness: defining “gamification”. In: *Proceedings of the 15th International Academic MindTrek Conference*. Tampere: ACM, 2011.

KAPP, Karl M. *The gamification of learning and instruction: game-based methods and strategies for training and education*. San Francisco: Pfeiffer, 2012.

KASPERSKY. *Pesquisa sobre privacidade e dados no Brasil*. 2023. Disponível em: <https://www.kaspersky.com.br>. Acesso em: 29 mar. 2026.

KASPERSKY. *Security Bulletin 2024*. Moscou: Kaspersky, 2024. Disponível em: <https://www.kaspersky.com/resource-center>. Acesso em: 29 mar. 2026.

NORTONLIFELOCK. *Norton Cyber Safety Insights Report*. 2023. Disponível em: <https://us.norton.com>. Acesso em: 29 mar. 2026.

WHITMAN, Michael E.; MATTORD, Herbert J. *Principles of information security*. 6. ed. Boston: Cengage Learning, 2018.