INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO

ADRIAN PESSOA NERY

PLATAFORMA EDUCATIVA PARA MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL

SALGUEIRO, 2025

ADRIAN PESSOA NERY

PLATAFORMA EDUCATIVA PARA MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Tecnólogo em Sistemas para Internet no Instituto Federal Sertão - Campus Salgueiro.

Orientador: Gustavo Sanchez

SALGUEIRO, 2025

Dados Internacionais de Catalogação na Publicação (CIP)

N443 Nery, Adrian Pessoa.

PLATAFORMA EDUCATIVA PARA MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL / Adrian Pessoa Nery. - Salgueiro, 2025.
35 f. : il.

Trabalho de Conclusão de Curso (Sistemas para Internet) -Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, Campus Salgueiro, 2025.
Orientação: Prof. Dr. Gustavo Freitas Sanchez.

1. Desenvolvimento de software. 2. Engenharia Social. 3. Educação Digital. 4. Cibersegurança. 5. Aplicativos Mobile. I. Título.

CDD 005.2

Gerado automaticamente pelo sistema Geficat, mediante dados fornecidos pelo(a) autor(a)

ADRIAN PESSOA NERY

PLATAFORMA EDUCATIVA PARA MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Tecnólogo em Sistemas para Internet no Instituto Federal Sertão - Campus Salgueiro.

BANCA EXAMINADORA

Prof. Gustavo Sanchez. Orientador(a)

IFSertãoPE – Campus Salgueiro

Prof. Francenila Rodrigues

IFSertãoPE – Campus Salgueiro

Prof. Francisco Junio Da Silva Fernandes

IFSertãoPE – Campus Salgueiro

SALGUEIRO, 2025

Dedico este trabalho à minha família e amigos, que sempre me apoiaram e incentivaram, bem como aos futuros leitores e pesquisadores que poderão se beneficiar dos conhecimentos aqui apresentados.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me guiar, ao meu orientador pelo suporte e paciência, ao Instituto Federal Sertão Pernambucano Campus Salgueiro pela oportunidade de crescimento profissional e pessoal. Dedico a todos aqueles que em algum momento dessa minha jornada me ajudaram de alguma forma, sou grato por tudo e todos. Queria agradecer aos professores por me guiar nos estudos, a tia Lineide por todo o carinho que ela teve por mim, aos meus amigos por compartilharem momentos de diversão e estudos. Não posso deixar de lado o esporte tênis de mesa pois muitas vezes me ajudou a tirar o estresse diário e me proporcionou amigos incríveis, sem vocês e sem o tênis de mesa talvez eu já tivesse desistido do curso.

“A proteção da informação não depende apenas de tecnologia, mas também do treinamento e conscientização das pessoas que lidam com dados sensíveis.” (Stallings, 2019)

RESUMO

Este trabalho apresenta o desenvolvimento de uma plataforma educativa voltada para a conscientização sobre ataques de phishing, com o objetivo de auxiliar usuários na identificação e prevenção desse tipo de ameaça. A solução foi projetada utilizando design centrado no usuário, implementada com React Native e Expo no frontend e Django Rest Framework no backend, garantindo integração eficiente e persistência de dados com SQLite. A plataforma oferece cadastro e autenticação de usuários, módulos de estudo, quizzes interativos e simulações práticas, permitindo aprendizado contínuo e feedback imediato. Foram realizados testes internos de navegação, autenticação, execução de quizzes e armazenamento de resultados, que confirmaram a estabilidade e funcionalidade do sistema. O trabalho demonstra a viabilidade técnica e pedagógica da solução e estabelece uma base para futuras melhorias, incluindo testes com usuários reais, expansão de conteúdo e otimização de acessibilidade, reforçando sua relevância no contexto da educação em segurança digital.

Palavras-chave: Phishing; Engenharia Social; Cibersegurança; Educação Digital; Aplicativos Mobile

ABSTRACT

This work presents the development of an educational platform aimed at raising awareness about phishing attacks, with the goal of helping users identify and prevent this type of threat. The solution was designed using a user-centered approach and implemented with React Native and Expo for the frontend, and Django Rest Framework for the backend, ensuring efficient integration and data persistence through SQLite. The platform offers user registration and authentication, learning modules, interactive quizzes, and practical simulations, enabling continuous learning and immediate feedback. Internal tests were carried out to validate navigation, authentication, quiz execution, and data storage, confirming the system's stability and functionality. The project demonstrates the technical and pedagogical feasibility of the solution and establishes a foundation for future improvements, including usability tests with real users, content expansion, and accessibility optimization, reinforcing its relevance within the context of digital security education.

Keywords: Phishing; Social Engineering; Cybersecurity; Digital Education; Mobile Applications

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API – Application Programming Interface

IHC – Interação Humano-Computador

ISO – International Organization for Standardization

SQL/SQLite – Structured Query Language / Banco de Dados

UML – Unified Modeling Language

UX/UI – User Experience / User Interface

Sumário

1. INTRODUÇÃO

A engenharia social é uma das ameaças mais relevantes à segurança da informação na atualidade, caracterizando-se por técnicas de manipulação psicológica que induzem as vítimas a realizar ações ou revelar informações confidenciais. Diferentemente de ataques puramente técnicos, ela explora vulnerabilidades humanas, que muitas vezes são o elo mais fraco da cadeia de segurança (MITNICK; SIMON, 2003).

Entre as modalidades existentes, o *phishing* destaca-se como o ataque mais frequente e de maior impacto. Segundo a Kaspersky (2023), 28,5% dos brasileiros já foram vítimas de tentativas de *phishing*, com prejuízos significativos causados por links falsos e páginas de login fraudulentas. O *phishing* é particularmente perigoso por sua simplicidade de execução e alta taxa de sucesso, explorando a confiança e a desatenção das pessoas.

Nesse contexto, a conscientização do usuário final é essencial para reduzir a ocorrência de ataques. Schneier (2015) e Stallings (2020) reforçam que soluções tecnológicas, embora importantes, não são suficientes sem a educação do público. Este trabalho propõe o desenvolvimento de uma plataforma educativa gamificada focada exclusivamente na prevenção de ataques de *phishing*, oferecendo ao usuário um ambiente interativo, com simulações práticas, *quizzes* e conteúdos didáticos que ensinam a identificar e evitar esse tipo de ameaça.

2. FUNDAMENTAÇÃO TEÓRICA

A segurança da informação é uma disciplina voltada para a proteção de dados e sistemas contra acessos não autorizados, alterações indevidas e indisponibilidade de serviços. Segundo Stallings (2019), sua base está apoiada em quatro princípios fundamentais: confidencialidade, integridade, disponibilidade e autenticidade. No entanto, o fator humano permanece como o elo mais fraco dessa cadeia, e ataques de engenharia social exploram exatamente essa vulnerabilidade (MITNICK; SIMON, 2003).

2.1 Engenharia Social e Phishing

A engenharia social é um conjunto de técnicas que têm por objetivo manipular pessoas para que revelem informações confidenciais ou executem ações que comprometam sua própria segurança. Hadnagy (2018) classifica ataques como *phishing*, *pretexting* e *baiting* como os mais comuns, sendo o *phishing* um dos mais difundidos globalmente.

O phishing consiste no envio de mensagens fraudulentas — geralmente e-mails, SMS ou mensagens instantâneas — que se passam por instituições legítimas para enganar o usuário e levá-lo a clicar em links ou informar dados pessoais, como senhas e informações bancárias (CERT.br, 2023). No Brasil, a FEBRABAN (2023) reporta que mais de 70% dos golpes digitais registrados em 2023 envolveram algum tipo de engenharia social, sendo o phishing a modalidade mais prevalente.

A gravidade do phishing está na sua facilidade de execução e alto índice de sucesso. Schneier (2015) destaca que, ao comprometer a confiança do usuário, esse tipo de ataque pode resultar em roubo de credenciais, fraude financeira e até acesso a sistemas corporativos. Assim, iniciativas de educação e conscientização são tão importantes quanto barreiras técnicas de proteção, como filtros AntiSpam.

2.2 Interação Humano-Computador (IHC)

A Interação Humano-Computador (IHC) é uma área que estuda como os usuários interagem com sistemas computacionais e como projetar interfaces mais acessíveis, eficientes e intuitivas (BARBOSA; SILVA, 2010). Aplicar conceitos de IHC em plataformas educativas é essencial para que o público leigo compreenda conteúdos complexos, como a identificação de tentativas de phishing.

Os sistemas devem ser projetados considerando aspectos cognitivos e sociais do usuário, de forma a reduzir carga mental e apresentar informações de maneira clara. Isso é especialmente importante para conscientização em segurança digital, onde mensagens ambíguas podem comprometer o aprendizado.

2.3 Usabilidade em Sistemas Digitais

A usabilidade refere-se à facilidade com que um sistema pode ser utilizado para atingir objetivos de forma eficaz e satisfatória (NIELSEN, 1994). A norma ISO 9241-210 (2010) define que o design centrado no usuário deve considerar suas necessidades, contexto e limitações, garantindo que o sistema seja intuitivo e promova uma experiência positiva.

No caso desta plataforma, a usabilidade garante que usuários não técnicos consigam navegar, realizar quizzes e compreender os resultados sem dificuldade. Um design bem planejado reduz barreiras de aprendizado e aumenta o engajamento do público.

2.4 Experiência do Usuário (UX) e Interface do Usuário (UI)

A Experiência do Usuário (UX) vai além da usabilidade, envolvendo aspectos emocionais e subjetivos, como satisfação, confiança e percepção de valor (GARRETT, 2011). A Interface do Usuário (UI) diz respeito aos elementos visuais — cores, ícones, tipografia — e à maneira como eles são organizados (ROGERS; SHARP; PREECE, 2013).

Uma boa combinação de UX e UI é fundamental para que o usuário se sinta confiante durante o uso da plataforma, aprenda de forma natural e tenha motivação para continuar explorando o conteúdo. No contexto da conscientização sobre phishing, uma interface bem projetada pode simular cenários reais de forma convincente, ajudando o usuário a reconhecer padrões de ataques em situações do dia a dia.

2.5 Gamificação e Aprendizagem Interativa

A gamificação é o uso de elementos de jogos em contextos não lúdicos, com o objetivo de engajar e motivar usuários (DETERDING et al., 2011). Em ambientes educacionais, mecânicas como pontos, níveis, recompensas e feedback imediato tornam o aprendizado mais envolvente e menos passivo (KAPP, 2012).

No ensino de segurança digital, a gamificação tem grande potencial para reforçar comportamentos desejáveis, como analisar links antes de clicar ou identificar sinais de páginas falsas. Ao transformar o aprendizado em um processo interativo, a plataforma aumenta a probabilidade de retenção do conhecimento e promove uma mudança de comportamento, essencial para reduzir o sucesso de ataques de phishing.

2.6 Iniciativas Educativas Existentes

Diversas iniciativas já buscam conscientizar usuários sobre golpes digitais. A KnowBe4 e a Cofense (PhishMe) oferecem treinamentos corporativos com simulações de *phishing*, mas são soluções pagas e em inglês, o que limita o alcance para o público leigo. Plataformas como Coursera e Udemy disponibilizam cursos teóricos sobre segurança, mas com pouca interatividade.

No Brasil, o CERT.br oferece cartilhas gratuitas com dicas de segurança, porém em formato estático e sem recursos de simulação. As campanhas da FEBRABAN têm caráter pontual, alertando sobre golpes financeiros, mas não oferecem aprendizado contínuo.

Essas lacunas reforçam a necessidade de uma solução gratuita, interativa e *gamificada*, voltada especificamente para conscientizar sobre *phishing*, permitindo ao usuário experimentar cenários simulados e aprender de forma prática como se proteger.

3 METODOLOGIA

Este projeto caracteriza-se como uma pesquisa aplicada, de abordagem qualitativa e caráter exploratório, com o objetivo de gerar um produto funcional — uma plataforma educativa para conscientização sobre *phishing* — que possa ser utilizada em treinamentos e campanhas de prevenção.

A abordagem qualitativa permite uma análise aprofundada de aspectos como usabilidade e experiência do usuário, sem depender exclusivamente de métricas numéricas. O caráter exploratório é adequado, uma vez que o projeto apresenta um protótipo inicial que poderá ser aprimorado com base em *feedback* futuro.

3.1 Levantamento de Requisitos e Estudo Teórico

Foi realizada uma revisão bibliográfica sobre:

- Engenharia social, com ênfase em ataques de *phishing*;
- Estratégias de ensino digital e gamificação;
- Tecnologias multiplataforma para desenvolvimento mobile e APIs REST.

Com base nesse estudo, foram definidos os requisitos funcionais e não funcionais apresentados na Tabela 01.

Tabela 01 – Requisitos Funcionais e Não Funcionais da Plataforma Educativa

Tipo	ID	Requisito	Descrição
Funcional	RF01	Cadastro de Usuário	Permitir que novos usuários criem uma conta informando nome, e-mail e senha
Funcional	RF02	Autenticação	Permitir login e logout do usuário autenticado.
Funcional	RF03	Listagem de Cursos	Exibir cursos disponíveis na plataforma, com título e breve descrição.
Funcional	RF04	Acesso ao Conteúdo	Permitir que o usuário visualize o conteúdo educativo de cada curso.
Funcional	RF05	Quiz Interativo	Exibir perguntas, calcular pontuação e armazenar resultado para cada usuário.
Funcional	RF06	Simulação de Phishing	Apresentar cenários de ataque para treino e aprendizado prático.
Funcional	RF07	Armazenamento Local	Salvar o progresso do usuário no banco de dados local (SQLite).
Funcional	RF08	Feedback de Resultados	Exibir ao usuário a pontuação obtida e dicas de melhoria após cada quiz.
Não Funcional	RNF01	Usabilidade	Interface simples, intuitiva e responsiva, adequada a usuários leigos.
Não Funcional	RNF02	Portabilidade	O aplicativo deve ser compatível com Android e iOS.
Não Funcional	RNF03	Desempenho	Resposta rápida às requisições, com tempo de carregamento inferior a 3 segundos.
Não Funcional	RNF04	Segurança	Proteger dados de login com autenticação segura (Token) e evitar armazenamento de senhas em texto plano.
Não Funcional	RNF05	Escalabilidade	Permitir expansão futura para novos cursos, quizzes e integração com servidores em nuvem.

FONTE: Próprio autor (2025)

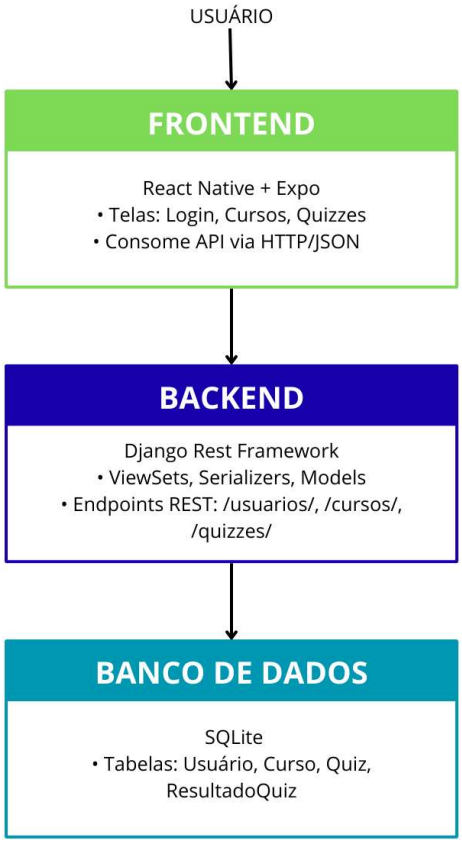
3.2 Planejamento e Design da Plataforma

O design da solução foi desenvolvido no Figma, com foco em clareza e UX. Foram aplicados princípios de design centrado no usuário, priorizando simplicidade, cores contrastantes e *feedback* visual imediato.

O *layout* foi estruturado em *cards* informativos, menus de navegação intuitivos e fluxos de tela otimizados, de acordo com as heurísticas de Nielsen (1994). Além disso, foram planejados elementos de gamificação, como pontuação, progresso e *feedback* instantâneo após *quizzes*, visando aumentar o engajamento do usuário.

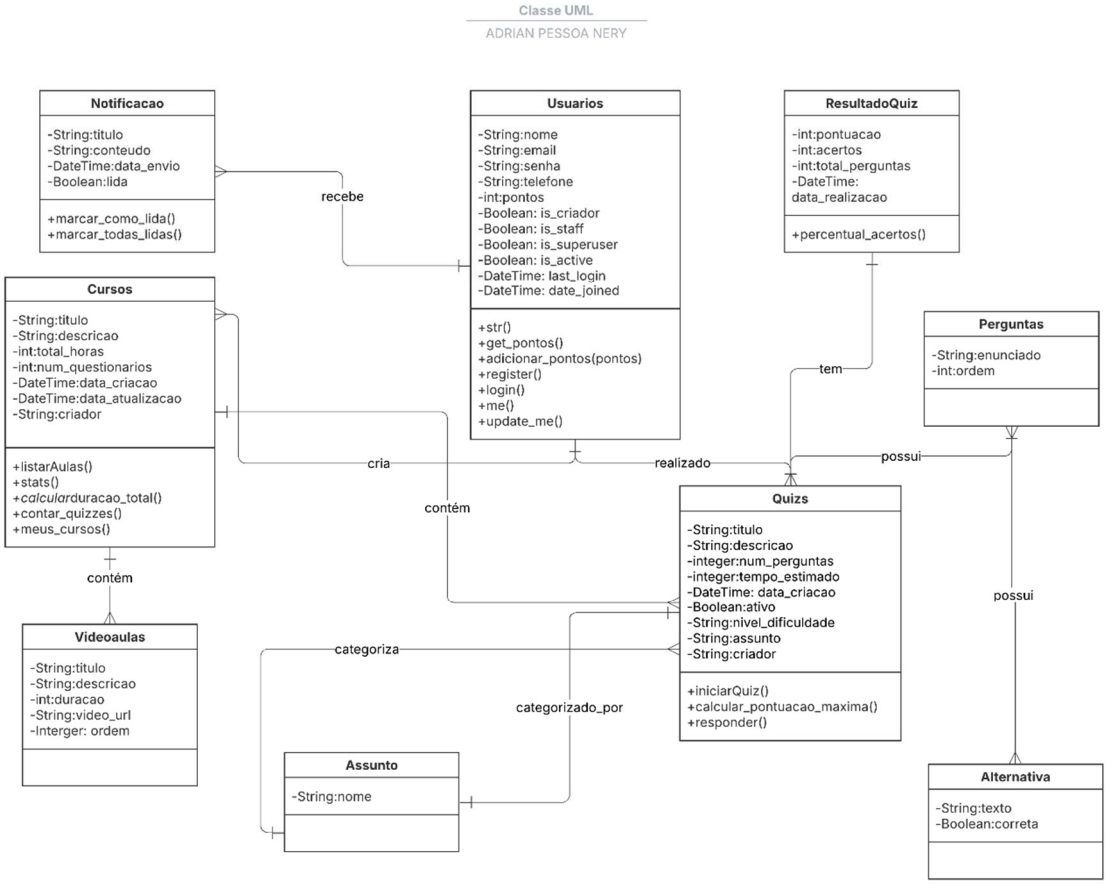
A arquitetura do sistema foi modelada em camadas (*frontend*, *backend* e banco de dados), e representada por diagramas de caso de uso e de classes, que descrevem as funcionalidades e a estrutura lógica da aplicação.

Figura 01 – Diagrama de Arquitetura em Camadas da Plataforma Educativa



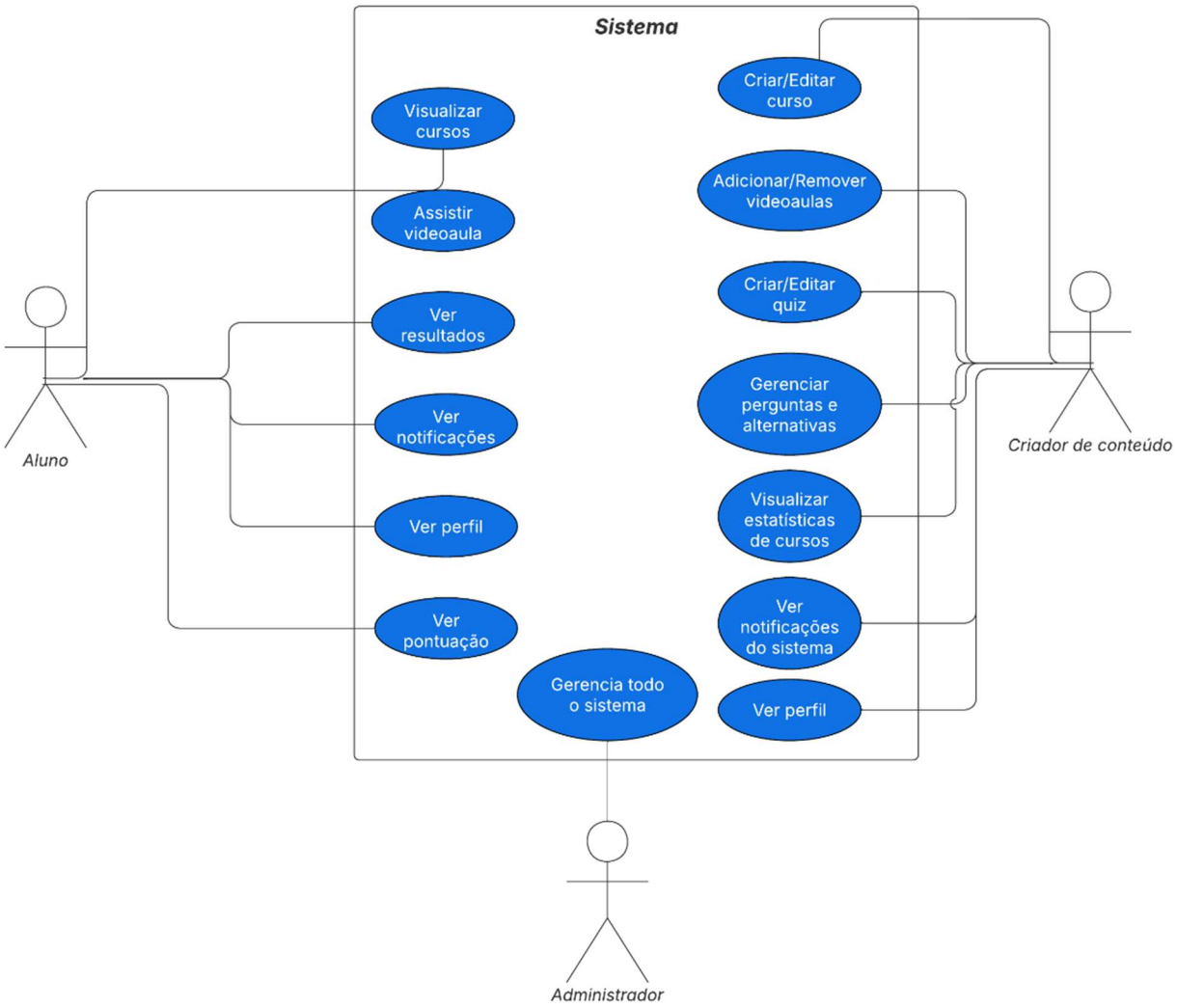
FONTE: Próprio autor (2025)

Figura 02 – Diagrama de Classes da Plataforma Educativa



FONTE: Próprio autor (2025)

Figura 03 – Diagrama de Caso de Uso da Plataforma Educativa



FONTE: Próprio autor (2025)

3.3 Tecnologias e Frameworks Utilizados

A escolha tecnológica visou garantir escalabilidade, portabilidade e facilidade de manutenção:

Tabela 02 – Tecnologias e Ferramentas Utilizadas

Tecnologia / Ferramenta	Função	Justificativa
Figma	Prototipação de interfaces	Permitiu criar e validar o design antes da implementação, reduzindo retrabalho.
React Native + Expo	Desenvolvimento do frontend mobile	Viabilizou desenvolvimento multiplataforma (Android/iOS) com rapidez e prototipagem ágil.
Django Rest Framework	Desenvolvimento do backend	Forneceu API REST robusta, com endpoints para autenticação, gerenciamento de usuários, cursos e quizzes.
SQLite	Banco de dados local	Utilizado para persistência de progresso do usuário e resultados dos quizzes no dispositivo.
TypeScript e Python	Linguagens de programação	Garantiram robustez no frontend e backend, respectivamente.
GitHub	Controle de versão	Facilitou versionamento, colaboração e rastreabilidade do código.

FONTE: Próprio autor (2025)

3.4 Desenvolvimento do Aplicativo

O desenvolvimento foi conduzido de forma iterativa, iniciando pela configuração do ambiente (instalação do Expo, criação do repositório no GitHub e configuração do *backend* com *Django Rest Framework*). Em seguida, as telas projetadas no *Figma* foram exportadas e adaptadas para *React Native*, com implementação da navegação e integração com a API REST. Após o desenvolvimento do *backend* — que incluiu a criação de modelos, serializers, views e endpoints — foi realizada a integração entre as camadas, garantindo a persistência de dados via SQLite. Por fim, testes internos foram executados para validar autenticação, navegação e execução dos *quizzes*.

3.4.1 Endpoints da API

A API foi documentada e disponibiliza os seguintes endpoints (Tabela 03):

Tabela 03 – Endpoints da API

Endpoints	Método	Descrição	Autenticação	Saída
/api/usuarios/register/	POST	Cria novo usuário.	Não requer	Dados do usuário + token
/api/usuarios/login/	POST	Faz login e gera token.	Não requer	Token + dados do usuário
/api/usuarios/me/	GET	Retorna dados do usuário logado.	Requer	JSON com dados do usuário
/api/usuarios/update_me/	PUT	Atualiza perfil do usuário.	Requer	Dados atualizados
/api/cursos/	GET	Lista cursos.	Requer	Lista de cursos
/api/quizzes/	GET	Lista quizzes	Requer	Lista de quizzes
/api/quizzes/{id}/responder/	POST	Registra respostas e calcula pontuação.	Requer	Pontuação + feedback
/api/resultados/	GET	Lista resultados de quizzes do usuário.	Requer	Lista de resultados

FONTE: Próprio autor (2025)

3.5 Testes e Validação

Foram realizados testes internos pelo próprio desenvolvedor, com foco em:

- Navegação entre telas;
- Fluxo de autenticação (login, logout e cadastro de usuário);
- Consumo correto dos dados via API REST;
- Persistência de resultados no banco local (SQLite).

Testes com usuários reais não foram realizados nesta fase, mas estão planejados para etapas futuras, utilizando questionários e observação de uso para medir compreensão e engajamento.

3.6 Público-Alvo

O público-alvo inclui estudantes do ensino médio/técnico, profissionais iniciantes em tecnologia e usuários leigos que desejam aprender a identificar e evitar ataques de phishing de forma prática e interativa.

4. RESULTADOS E DISCUSSÃO

Nesta seção são apresentados os resultados obtidos com o desenvolvimento do protótipo da plataforma educativa voltada à mitigação de ataques de engenharia social. O protótipo foi implementado utilizando React Native, Expo e SQLite, com foco em oferecer uma experiência interativa, responsiva e gamificada para usuários leigos em segurança digital.

A seguir, descrevem-se as principais telas e funcionalidades implementadas.

4.1 Tela Inicial (Home)

Após realizar o login, o usuário é direcionado para a Tela Inicial (Home) (Figura 04), que representa o ponto de entrada da aplicação e concentra os principais recursos disponíveis. O design foi pensado para ser simples, organizado e intuitivo, facilitando a navegação do usuário.

Na parte superior, o usuário visualiza seu nome de perfil e possui acesso a uma barra de pesquisa, que permite buscar cursos, temas ou tags de interesse. Ao lado, há um ícone de notificações, que centraliza alertas importantes sobre novos cursos ou atividades.

A seção “Cursos em Alta” destaca os cursos mais relevantes e recentes da plataforma, apresentados em *cards* chamativos que incluem o título e uma breve descrição. Essa área funciona como um convite visual para que o usuário explore conteúdos em destaque.

Logo abaixo, a interface disponibiliza um menu de alternância (“Cursos” e “Quizzes”), que permite filtrar o conteúdo exibido de acordo com a preferência do usuário.

A seção “Aprenda na Prática” lista os questionários disponíveis, trazendo informações essenciais como:

- *Título do questionário;*
- *Breve descrição;*
- *Quantidade de perguntas;*
- *Tempo estimado de resolução;*

- *Tema associado (com tags destacadas).*

Já na seção “Aprenda com Videoaulas”, o usuário tem acesso direto a conteúdos audiovisuais, também apresentados em cards com título, descrição e categorias.

Por fim, a tela é complementada por um menu de navegação inferior, composto por ícones que dão acesso rápido às principais áreas do aplicativo: Home, Videoaulas, Quizzes/Notícias e Perfil do Usuário.

Assim, a Tela Inicial não apenas apresenta os cursos e atividades, mas também funciona como um painel central de interação, permitindo que o usuário explore diferentes recursos de forma dinâmica e agradável.

Figura 04 – Tela Inicial/Home

FONTE: Próprio autor (2025)

4.2 Tela de Cursos

A Tela de Cursos (Figura 05) é dedicada à apresentação detalhada dos conteúdos educacionais disponíveis na plataforma. Ela foi projetada para que o usuário possa navegar, filtrar e escolher os cursos que deseja realizar de forma clara e organizada.

Na parte superior, encontra-se o título da seção e uma barra de busca, que permite localizar cursos por palavras-chave, como assunto, tema ou nome do instrutor. Logo abaixo, há uma barra de filtros por categorias (ex.: “Todos”, “*Phishing*”, “*Spear Phishing*”, etc.), que facilita a organização do conteúdo e direciona o usuário aos cursos de seu interesse específico.

Cada curso é exibido em um card visual, contendo informações essenciais:

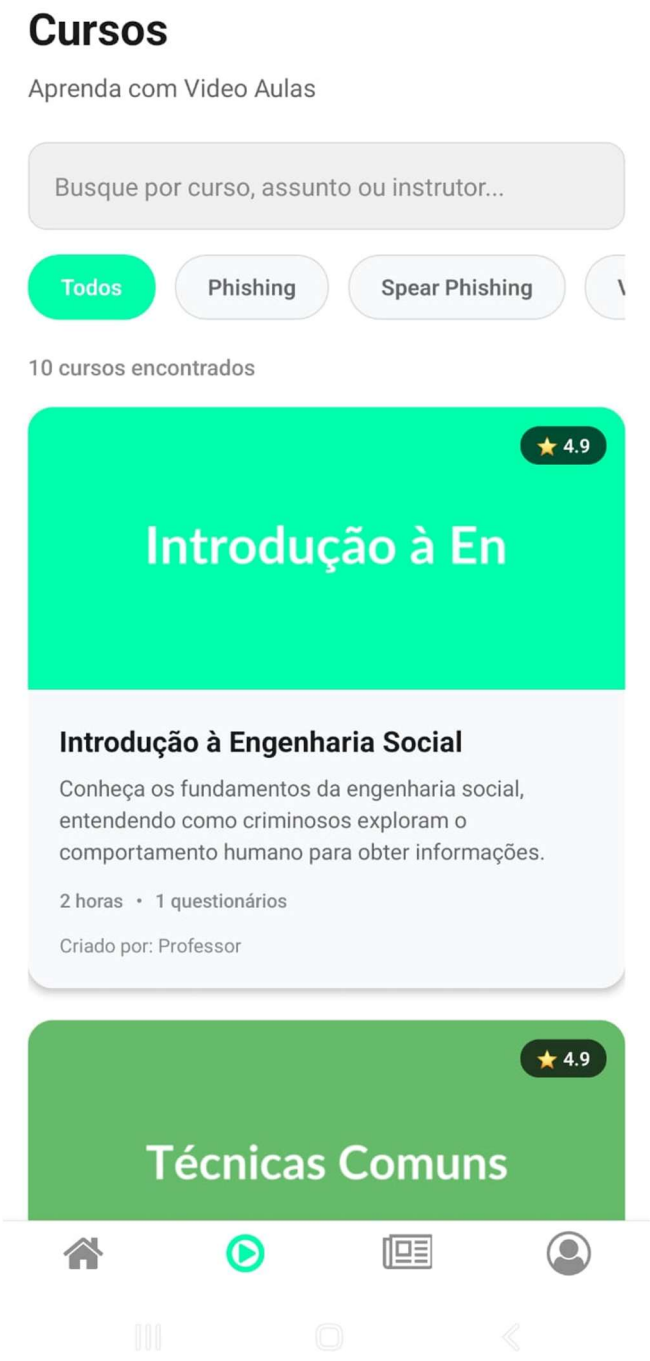
- **Título do curso**: destacado em uma faixa colorida, tornando a identificação rápida.
- **Descrição**: breve resumo dos objetivos e conteúdos do curso.
- **Carga horária estimada**: tempo médio necessário para a conclusão.
- **Quantidade de questionários associados**: indicando atividades práticas de fixação.
- **Avaliação por estrelas**: permitindo ao usuário identificar a qualidade do curso com base no feedback de outros participantes.
- **Nome do criador/instrutor**: reforçando a credibilidade do conteúdo.

Além disso, a tela organiza todos os cursos encontrados, exibindo também o total disponível para consulta, o que transmite ao usuário a amplitude do material oferecido.

Na parte inferior, o menu de navegação global é mantido, permitindo alternar rapidamente entre as seções Home, Cursos, Quizzes/Notícias e Perfil.

Essa tela cumpre a função de catálogo de aprendizagem, sendo o espaço onde o usuário descobre, compara e escolhe os cursos mais relevantes para seu desenvolvimento.

Figura 05 – Tela de Cursos



FONTE: Próprio autor (2025)

4.3 Tela de Quiz

A Tela de Quizzes (Figura 06) é o espaço voltado para a prática dos conhecimentos adquiridos, permitindo que o usuário teste suas habilidades e fixe o conteúdo estudado.

Na parte superior, há uma barra de busca, que possibilita localizar quizzes por tema, assunto ou palavra-chave. Logo abaixo, a tela disponibiliza filtros de dificuldade (Todos, Fácil, Médio, Difícil) e filtros de status (Todos, Completos, Pendentes), permitindo ao usuário organizar os quizzes de acordo com seu nível de experiência ou progresso.

Cada quiz é apresentado em um *card* informativo, contendo:

- **Título**: identificação clara do tema do quiz.
- **Descrição**: breve explicação sobre os conceitos que serão abordados.
- **Indicador de dificuldade**: mostrando se o quiz é classificado como fácil, médio ou difícil.
- **Quantidade de perguntas** e **tempo estimado** para resolução.
- **Status de conclusão**: exibido com selo visual (“Concluído” ou “Pendente”).
- **Pontuação do usuário**: apresentada em percentual, com barra de progresso colorida, permitindo acompanhar o desempenho em cada atividade.

Essa tela é organizada para incentivar o estudo prático e dar retorno imediato ao usuário sobre sua performance, funcionando como um instrumento de avaliação contínua.

Assim como nas outras telas, o menu de navegação inferior é mantido, garantindo o acesso rápido a outras áreas da aplicação: Home, Cursos, Quizzes e Perfil do Usuário.

Dessa forma, a Tela de Quizzes representa um dos pontos centrais da plataforma, pois promove a consolidação do aprendizado por meio de desafios objetivos e medição de resultados.

Figura 06 – Tela de Quizzes

FONTE: Próprio autor (2025)

A tabela 04 demonstra uma análise entre Funcionalidades x Justificativa de Design

Tabela 04 – Funcionalidades e Justificativas de Design

Funcionalidade	Descrição	Justificativa	Conceito de UX/UI
Barra de Pesquisa	Buscar cursos e quizzes	Facilitar acesso rápido ao conteúdo	Visibilidade, controle do usuário
Cards de cursos	Exibir informações resumidas	Melhor organização visual	Clareza, consistência
Quizzes interativos	Testar conhecimento	Gamificação e engajamento	Feedback imediato, motivação
Menu inferior	Navegação rápida	Consistência e facilidade de uso	Navegação contínua, acessibilidade

FONTE: Próprio autor (2025)

4.4 Discussão dos Resultados

O protótipo demonstrou viabilidade técnica e funcional para atender aos objetivos do projeto. Os elementos de gamificação (pontuação, quizzes, progresso) e os conteúdos multimídia (vídeo aulas e textos) tornam o processo de aprendizado mais dinâmico e envolvente, facilitando a compreensão de conceitos complexos relacionados à engenharia social.

Apesar disso, algumas limitações ainda se destacam:

- **Ausência de testes com usuários reais**, o que impede avaliar completamente a eficácia da plataforma em termos de usabilidade, engajamento e retenção de conhecimento;
- **Base de dados de conteúdos ainda reduzida**, limitando a variedade de cenários e exercícios;
- **Funcionalidades avançadas**, como notificações *push* e integração com servidor remoto, não foram implementadas nesta fase.

Conforme apontam Nielsen (1993) e Rubin & Chisnell (2008), avaliações de usabilidade com usuários são essenciais para identificar problemas de interação,

medir eficiência, eficácia e satisfação, e validar se o sistema atende às necessidades do público-alvo. Esses estudos reforçam que testes com usuários não apenas apontam falhas técnicas, mas também evidenciam oportunidades de melhoria na experiência do usuário e na aprendizagem.

Portanto, a próxima etapa do projeto consistirá na condução de testes de usabilidade com usuários reais, visando:

- Coletar feedback qualitativo e quantitativo sobre a interface e funcionalidades;
- Identificar pontos de melhoria na navegação e interação com os conteúdos;
- Avaliar a eficácia dos elementos de gamificação na aprendizagem;
- Ajustar a plataforma para melhor atender às expectativas e necessidades do público-alvo.

Dessa forma, espera-se que essas avaliações subsidiem ajustes que aprimorem a experiência do usuário e aumentem a efetividade da plataforma como ferramenta de conscientização sobre ataques de engenharia social.

5. CONCLUSÃO

O presente trabalho teve como objetivo o desenvolvimento de uma plataforma educativa voltada para a conscientização sobre ataques de phishing, oferecendo aos usuários um ambiente interativo para aprendizado e prática. A escolha por focar exclusivamente nesse tipo de ataque atendeu à necessidade de delimitar o escopo da pesquisa, permitindo aprofundar a análise e a construção de cenários mais realistas e eficazes para a prevenção desse tipo de ameaça.

Os resultados obtidos demonstraram que o protótipo desenvolvido é tecnicamente viável e cumpre o propósito para o qual foi concebido. A implementação contemplou funcionalidades essenciais, como cadastro e autenticação de usuários, listagem de cursos, quizzes interativos e armazenamento de progresso, garantindo que o usuário possa aprender de forma contínua e acompanhar sua evolução. A integração bem-sucedida entre o frontend, desenvolvido em React Native com Expo,

e o backend, construído com Django Rest Framework, mostrou-se eficiente, com comunicação estável e desempenho satisfatório.

A análise dos testes internos indicou que a aplicação é estável e apresenta boa experiência de uso, ainda que seja necessária a realização de testes com usuários reais para validação completa da usabilidade e do impacto pedagógico da plataforma. Essa etapa futura permitirá ajustar fluxos de navegação, identificar pontos de melhoria e medir de forma objetiva o grau de conscientização adquirido pelos participantes após a utilização da ferramenta.

Entre as principais limitações identificadas, destacam-se a ausência de testes com usuários finais e a necessidade de ampliação do conteúdo educativo, com mais exemplos de ataques e simulações interativas. Sugere-se, para trabalhos futuros, a implementação de testes automatizados para assegurar maior robustez ao código, a inclusão de novos módulos educativos sobre outras formas de engenharia social, melhorias de acessibilidade para contemplar usuários com diferentes necessidades e a implantação da solução em ambiente de produção com suporte a múltiplos dispositivos.

Conclui-se que a plataforma proposta representa uma contribuição prática e relevante para a área de segurança da informação, especialmente no campo da educação digital. Ao proporcionar ao usuário uma experiência gamificada e interativa, o sistema não apenas transmite conhecimento teórico, mas também estimula a prática e o reconhecimento de ameaças em situações simuladas, preparando-o para responder de forma mais assertiva no mundo real. Dessa forma, o trabalho cumpre seu objetivo de servir como ferramenta de apoio na mitigação de ataques de phishing e estabelece uma base sólida para evoluções futuras.

6. REFERÊNCIAS

BARBOSA, Simone Diniz Junqueira; SILVA, Bruno Santana da. *Interação Humano-Computador*. Rio de Janeiro: Elsevier, 2010.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. *Cartilha de Segurança para Internet*. 2023. Disponível em: https://cartilha.cert.br/. Acesso em: 15 set. 2025.

DETERDING, Sebastian *et al.* From Game Design Elements to Gamefulness: Defining "Gamification". In: *Proceedings of the 15th International Academic MindTrek Conference*. Tampere, 2011. p. 9–15.

DJANGO SOFTWARE FOUNDATION. *Django REST Framework Documentation*. Disponível em: https://www.django-rest-framework.org/. Acesso em: 20 set. 2025.

EXPO. *Expo Documentation*. Disponível em: https://docs.expo.dev/. Acesso em: 20 set. 2025.

FEBRABAN – Federação Brasileira de Bancos. *Relatório de Prevenção a Fraudes Digitais*. 2023. Disponível em: https://www.febraban.org.br/. Acesso em: 15 set. 2025.

FIGMA. *Figma – Collaborative Interface Design Tool*. Disponível em: https://www.figma.com/. Acesso em: 20 set. 2025.

GARRETT, Jesse James. *The Elements of User Experience: User-Centered Design for the Web and Beyond*. 2. ed. Berkeley: New Riders, 2011.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2008.

GITHUB. *GitHub: Where the World Builds Software*. Disponível em: https://github.com/. Acesso em: 20 set. 2025.

HADNAGY, Christopher. *Social Engineering: The Science of Human Hacking*. 2. ed. Indianapolis: Wiley, 2018.

KAPP, Karl M. *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education*. San Francisco: Pfeiffer, 2012.

KASPERSKY LAB. *Relatório de Cibersegurança no Brasil – Phishing*. 2023. Disponível em: https://www.kaspersky.com.br. Acesso em: 15 set. 2025.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Metodologia científica*. 7. ed. São Paulo: Atlas, 2003.

META. *React Native Documentation*. Disponível em: https://reactnative.dev/. Acesso em: 20 set. 2025.

MITNICK, Kevin; SIMON, William. *A arte de enganar: lições de um hacker mestre sobre segurança da informação*. São Paulo: Pearson, 2003.

NIELSEN, Jakob. *Usability Engineering*. Boston: Academic Press, 1994.

RUBIN, Jeffrey; CHISNELL, Dana. *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests*. 2. ed. Indianapolis: Wiley, 2008.

SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company, 2015.

SQLITE. *SQLite Database Engine*. Disponível em: https://www.sqlite.org/. Acesso em: 20 set. 2025.

STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 8. ed. Boston: Pearson, 2019.