

Campus Porto Velho Zona Norte
Coordenação do Curso de Tecnologia em Sistemas para Internet

LUIZ FELIPE ALBUQUERQUE BICALHO

**TÍTULO: CONECTE E CERTIFIQUE: UM PROTÓTIPO DE APLICAÇÃO PARA
EMISSÃO E GESTÃO DE CERTIFICADOS DIGITAIS COM FOCO EM
SEGURANÇA E USABILIDADE**

PORTO VELHO

2025

LUIZ FELIPE ALBUQUERQUE BICALHO

**TÍTULO: CONECTE E CERTIFIQUE: UM PROTÓTIPO DE APLICAÇÃO PARA
EMISSÃO E GESTÃO DE CERTIFICADOS DIGITAIS COM FOCO EM
SEGURANÇA E USABILIDADE**

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus Porto Velho Zona Norte*, como requisito parcial para obtenção do grau de Curso superior de Tecnologia, junto ao Curso de Sistemas para Internet sob a orientação do professor Ivanilse Calderon.

PORTO VELHO

2025

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Bicalho, Luiz Felipe Albuquerque.
Conecte e certifique: protótipo para emissão e gestão de certificados digitais / Luiz Felipe Albuquerque Bicalho. - Porto Velho, 2025.
15 f. : il.

Orientador(a): Profª Me. Maria Ivanilse Calderon Ribeiro.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Sistemas para Internet) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2025.

1. Certificados digitais . 2. Design thinking. 3. Segurança da informação. 4. Prototipação de software. I. Ribeiro, Maria Ivanilse Calderon (orient.). II. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. III. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-11/914

LUIZ FELIPE ALBUQUERQUE BICALHO

**TÍTULO: CONECTE E CERTIFIQUE: UM PROTÓTIPO DE APLICAÇÃO PARA
EMISSÃO E GESTÃO DE CERTIFICADOS DIGITAIS COM FOCO EM
SEGURANÇA E USABILIDADE**

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus Porto Velho Zona Norte*, como requisito parcial para obtenção do grau de Curso superior de Tecnologia, junto ao Curso de Sistemas para Internet sob a orientação do professor Ivanilse Calderon.

Aprovado em: 03/07/2025 pela banca examinadora.

Profa. Mariela Tamada

Prof. Alan Jhone

Prof. Tiago Lopes

Profa. Ivanilse Calderon Ribeiro

TÍTULO: CONECTE E CERTIFIQUE: UM PROTÓTIPO DE APLICAÇÃO PARA EMISSÃO E GESTÃO DE CERTIFICADOS DIGITAIS COM FOCO EM SEGURANÇA E USABILIDADE

RESUMO: Este trabalho apresenta o desenvolvimento de um protótipo de aplicação móvel, denominado Conecte e Certifique, para a emissão, armazenamento e validação de certificados digitais. A introdução aborda a crescente necessidade de sistemas de certificação digital seguros frente à vulnerabilidade e falsificação de documentos, estabelecendo o objetivo de projetar uma solução que integre praticidade, segurança e acessibilidade. A metodologia adotada foi o Design Thinking, fundamentado no modelo Duplo Diamante, que orientou desde a exploração do problema até a entrega de uma solução centrada no usuário. Os procedimentos metodológicos incluíram pesquisa quantitativa, construção de personas, mapas de empatia e jornadas de usuário para definir os requisitos do sistema. Como resultados, apresenta-se um protótipo de alta fidelidade com funcionalidades de personalização, geração de certificados em múltiplos formatos e uma arquitetura técnica proposta que utiliza assinaturas digitais no padrão PAdES para garantir autenticidade e integridade. Conclui-se que o protótipo atende às demandas identificadas, oferecendo uma base robusta para o desenvolvimento de um sistema completo, e sugere-se como trabalhos futuros a implementação da arquitetura proposta e a exploração de tecnologias como blockchain para aprimorar a rastreabilidade.

PALAVRAS-CHAVE: certificados digitais; design thinking; segurança da informação; usabilidade; prototipação de software.

ABSTRACT: This paper presents the development of a mobile application prototype, called Conecte e Certifique, for issuing, storing, and validating digital certificates. The introduction addresses the growing need for secure digital certification systems in the face of document vulnerability and forgery, establishing the objective of designing a solution that integrates practicality, security, and accessibility. The methodology adopted was Design Thinking, based on the Double Diamond model, which guided the process from problem exploration to the delivery of a user-centered solution. Methodological procedures included quantitative research, construction of personas, empathy maps, and user journeys to define system requirements. As a result, a high-fidelity prototype is presented with features for customization, certificate generation in multiple formats, and a proposed technical architecture that uses digital signatures in the PAdES standard to ensure authenticity and integrity. It is concluded that the prototype meets the identified demands, offering a robust basis for the development of a complete system, and future work is suggested, such as implementing the proposed architecture and exploring technologies like blockchain to enhance traceability.

KEYWORDS: digital certificates; design thinking; information security; usability; software prototyping.

1. INTRODUÇÃO

A transformação digital tem redefinido processos em diversos setores, incluindo o educacional e o corporativo. Nesse cenário, a emissão e validação de certificados digitais consolidam-se como uma prática essencial para a comprovação de competências e a rastreabilidade de qualificações de forma eletrônica. Contudo, a transição do meio físico para o digital introduz desafios significativos relacionados à segurança e autenticidade dos documentos emitidos. A integridade de um certificado digital é a sua característica mais crítica, pois garante que o documento não foi alterado desde a sua emissão, um pilar fundamental para a confiança no processo (ASSUNÇÃO; SANTOS, 2021).

Sistemas tradicionais de geração de certificados frequentemente empregam mecanismos de segurança frágeis, como tokens de autenticação estáticos, tornando-os suscetíveis a ataques que podem comprometer a validade dos documentos. A falsificação de diplomas e certificados é uma preocupação crescente, com estudos apontando para a detecção de milhares de documentos fraudulentos em curtos períodos, o que evidencia a urgência por sistemas mais robustos e confiáveis. Este contexto de vulnerabilidade reforça a importância da adoção de tecnologias como assinaturas digitais e mecanismos de validação automatizada, que assegurem a autenticidade e a integridade das informações contidas nos certificados (GOMES; ALMEIDA, 2022).

Diante desses desafios, os usuários — tanto indivíduos quanto instituições — demandam soluções que sejam simultaneamente práticas, seguras e acessíveis. O desenvolvimento de aplicações dedicadas à gestão de certificados digitais surge como uma alternativa promissora, oferecendo funcionalidades como geração automática, armazenamento centralizado e validação instantânea. Tais soluções não apenas mitigam os riscos de fraude, mas também eliminam a dependência de documentos físicos e promovem uma experiência de usuário mais conveniente e eficiente.

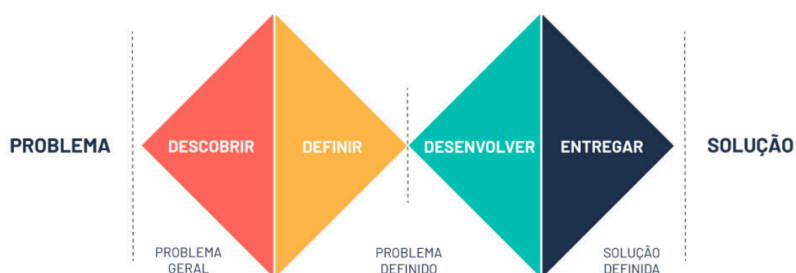
Este artigo, portanto, apresenta os resultados de um Trabalho de Conclusão de Curso (TCC) cujo objetivo foi propor e desenvolver um protótipo de alta fidelidade para uma aplicação móvel, o "Conecte e Certifique", voltado à emissão, ao armazenamento e à validação de certificados digitais. A proposta busca atender às demandas contemporâneas por segurança e praticidade, oferecendo uma solução que garanta a integridade e a autenticidade dos certificados por meio de uma arquitetura tecnologicamente fundamentada. Com isso, pretende-se contribuir para a modernização dos processos de certificação digital, fortalecendo a confiança nos documentos emitidos por instituições educacionais e outras organizações.

2. METODOLOGIA

Para nortear o desenvolvimento do projeto, foi adotada a metodologia Design Thinking (DT), uma abordagem estruturada para a inovação e resolução de problemas complexos amplamente aplicada em projetos de Experiência do Usuário (UX) e Interface do Usuário (UI). O DT posiciona as pessoas no centro do processo de desenvolvimento, priorizando a compreensão profunda de suas necessidades, dores e expectativas (VIANNA et al., 2012).

A estrutura do DT foi operacionalizada por meio do modelo Duplo Diamante (Double Diamond), representado na Figura 1. Desenvolvido pelo Design Council do Reino Unido, este modelo é iterativo e não linear, alternando entre momentos de pensamento divergente (para explorar o problema amplamente) e convergente (para focar em soluções específicas). Essa flexibilidade o torna ideal para projetos que demandam adaptação e feedback contínuo (BROWN, 2008).

Figura 1 - Modelo Duplo Diamante

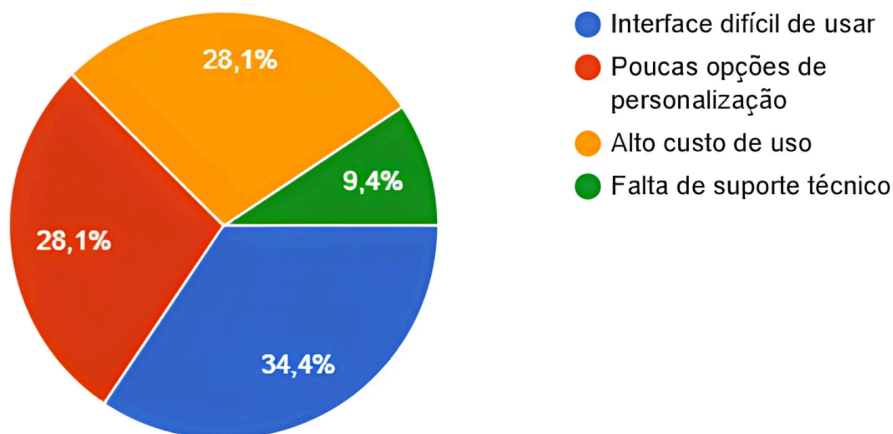


Fonte: Adaptado de Design Council (2024).

O processo foi organizado em quatro fases distintas:

Fase 1: Descobrir (Divergência): Etapa inicial focada na imersão no contexto do problema para identificar necessidades e oportunidades. Para isso, foi aplicada uma pesquisa quantitativa por meio de questionários, visando coletar dados primários sobre as dificuldades enfrentadas pelos usuários com os sistemas de certificação existentes. Os principais resultados dessa pesquisa são apresentados no Gráfico 1.

Gráfico 1 - Principais problemas relatados pelos usuários com ferramentas de certificação



Fonte: Elaborado pelos autores (2025).

Fase 2: Definir (Convergência): Nesta fase, as informações coletadas na etapa anterior foram organizadas e analisadas para proporcionar uma definição clara e focada do problema a ser resolvido. Ferramentas como a construção de Personas, Mapas de Empatia e a Jornada do Usuário foram utilizadas para sintetizar os achados e delimitar o escopo da solução.

Fase 3: Desenvolver (Divergência): Momento dedicado à ideação e ao desenvolvimento de múltiplas soluções possíveis para o problema definido. Realizou-se a análise de concorrentes, a elaboração de wireframes de baixa fidelidade e a definição de um guia de estilo (Style Guide) para orientar a identidade visual da aplicação.

Fase 4: Entregar (Convergência): Etapa final na qual a solução mais promissora foi refinada, testada e materializada em um protótipo de alta fidelidade. Este protótipo, desenvolvido na plataforma Figma, representa a solução funcional e interativa do aplicativo "Conecte e Certifique", alinhado ao guia de estilo e pronto para validação com usuários.

Cada fase foi suportada por ferramentas específicas que garantiram uma transição lógica e fundamentada da identificação do problema ao desenvolvimento da solução final.

3. RESULTADOS E DISCUSSÃO

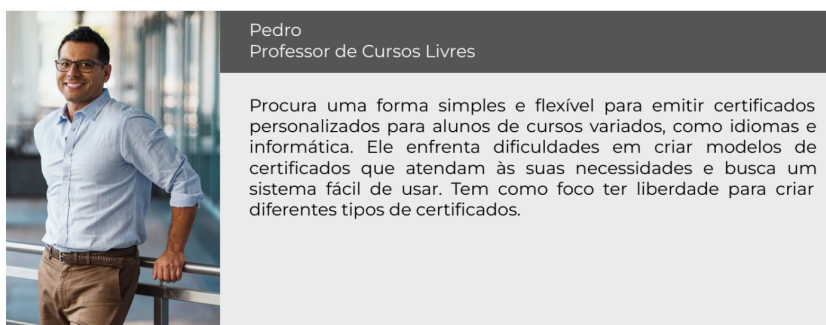
Nesta seção, são apresentados os artefatos gerados durante o projeto, que culminaram na concepção do protótipo e na proposta de sua arquitetura técnica.

3.1. ARTEFATOS DE UX DESIGN

A construção dos artefatos de UX foi fundamental para garantir que a solução fosse centrada nas necessidades do usuário.

Persona: A persona "Pedro" (Figura 2) foi desenvolvida para representar o usuário-alvo principal: um professor de cursos livres que busca uma maneira simples e flexível de emitir certificados personalizados. Pedro enfrenta dificuldades com a falta de customização das ferramentas atuais e valoriza a facilidade de uso e a liberdade para criar diferentes tipos de certificados. A criação de personas é uma técnica consolidada para delimitar modelos mentais que guiam o design (NUNES; QUARESMA, 2018).

Figura 2 - Representação da persona desenvolvida



https://cdn.pixabay.com/photo/2020/11/30/1721/businessman-5791566_1280.jpg

Fonte: Elaborado pelos autores (2025).

Mapa de Empatia: Complementando a persona, o mapa de empatia (Figura 3) aprofundou a compreensão sobre o universo de Pedro. O mapa revelou que ele: pensa e sente a necessidade de praticidade e se preocupa com sua imagem profissional; vê ferramentas caras e com pouca personalização; fala e faz pesquisas por soluções gratuitas e tutoriais online; e escuta sobre a importância de ter um design profissional. Suas dores centram-se em custos, tempo e complexidade, enquanto seus ganhos estão ligados à economia de tempo e ao reconhecimento profissional.

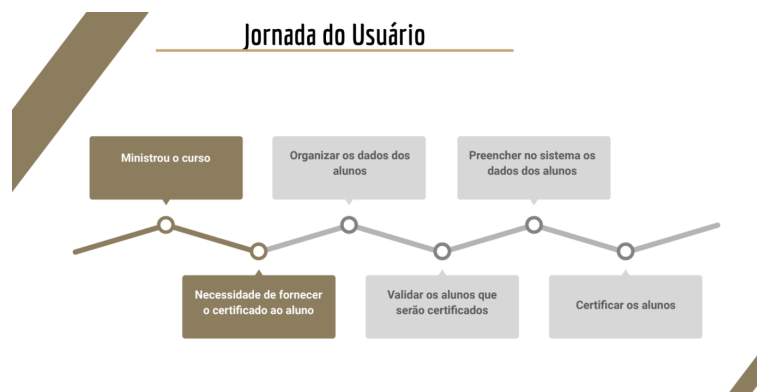
Figura 3 - Mapa de empatia do usuário



Fonte: Elaborado pelos autores (2025).

Jornada do Usuário: O mapeamento da jornada do usuário (Figura 4) ilustrou as etapas, os pontos de contato e as emoções de Pedro ao longo do processo de certificação, desde "ministrar o curso" até a "certificação dos alunos", destacando a "necessidade de fornecer o certificado" como um ponto crítico. Essa análise permitiu identificar gargalos e oportunidades de melhoria na experiência do usuário.

Figura 4 - Mapa da jornada do usuário



Fonte: Elaborado pelos autores (2025).

3.2. PROPOSTA DE ARQUITETURA TÉCNICA E DE SEGURANÇA

Para além do design da interface, a robustez de uma aplicação de certificados digitais reside em sua arquitetura técnica e de segurança. A seguir, detalha-se uma proposta de arquitetura para o "Conecte e Certifique", projetada para garantir a integridade, autenticidade e disponibilidade dos dados.

A arquitetura pode ser estruturada em um modelo de três camadas: front-end (aplicação móvel), back-end (servidor da aplicação) e a camada de persistência (banco de dados).

Front-end: Para o aplicativo móvel, sugere-se o uso de um framework multiplataforma como React Native ou Flutter. Essa escolha otimiza o desenvolvimento, permitindo a manutenção de uma única base de código para os sistemas operacionais Android e iOS, o que reduz custos e tempo de desenvolvimento (SILVA; LIMA, 2021). O front-end seria responsável por renderizar as interfaces apresentadas no protótipo e se comunicar com o back-end via uma API RESTful.

Back-end: O servidor da aplicação, atuando como o núcleo do sistema, pode ser desenvolvido em Node.js com o framework Express.js. Essa tecnologia é conhecida por sua alta performance em operações de I/O (entrada/saída), sendo ideal para gerenciar as requisições do aplicativo, processar a geração dos certificados e aplicar as assinaturas digitais (BARBOSA, <https://www.google.com/search?q=2019>). A comunicação entre cliente e servidor deve ser obrigatoriamente protegida com o protocolo HTTPS (SSL/TLS) para criptografar os dados em trânsito e prevenir ataques do tipo man-in-the-middle.

Persistência de Dados: Um banco de dados relacional como o PostgreSQL é recomendado para armazenar as informações de usuários, cursos e metadados dos certificados. A natureza estruturada do PostgreSQL e seu suporte a transações ACID (Atomicidade, Consistência, Isolamento e Durabilidade) são fundamentais para garantir a consistência dos dados (OLIVEIRA, 2020).

3.3. MECANISMOS DE SEGURANÇA PARA CERTIFICADOS

A funcionalidade mais crítica da aplicação é a garantia de autenticidade e integridade dos certificados. Para isso, o mecanismo de assinatura digital é central.

A proposta é que, no momento da emissão, o back-end gere o certificado em formato PDF e aplique uma assinatura digital no padrão PAdES (PDF Advanced Electronic Signatures). Esse padrão, regulamentado no Brasil pela ICP-Brasil, incorpora a assinatura eletrônica ao próprio documento PDF, incluindo um carimbo de tempo que atesta a data e a hora exatas da assinatura (ITI, 2021). O processo ocorreria da seguinte forma:

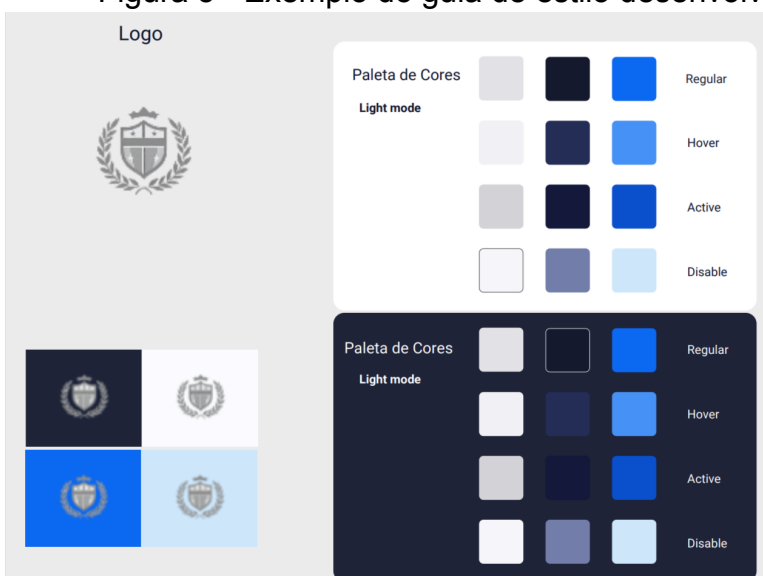
1. O servidor gera o PDF do certificado com os dados do aluno e do curso.
2. Um hash criptográfico (e.g., SHA-256) do conteúdo do PDF é calculado.
3. Esse hash é assinado com a chave privada da instituição emissora (armazenada de forma segura em um Hardware Security Module - HSM).
4. A assinatura digital resultante, junto ao certificado digital da instituição, é embutida no arquivo PDF.

Qualquer tentativa de alteração do PDF após a assinatura invalidaria o hash, tornando a fraude facilmente detectável por qualquer software validador de assinaturas, como o Verificador de Conformidade do ITI. Esta abordagem confere validade jurídica e um alto grau de confiabilidade aos documentos emitidos pela plataforma (GOMES; ALMEIDA, 2022).

3.4. PROTÓTIPO DE ALTA FIDELIDADE

Os resultados culminaram no protótipo de alta fidelidade, que materializa as funcionalidades do sistema. Para garantir consistência visual e funcional, foi desenvolvido um guia de estilo (Figura 5), estabelecendo padrões para a interface, como paleta de cores, tipografia e componentes.

Figura 5 - Exemplo do guia de estilo desenvolvido

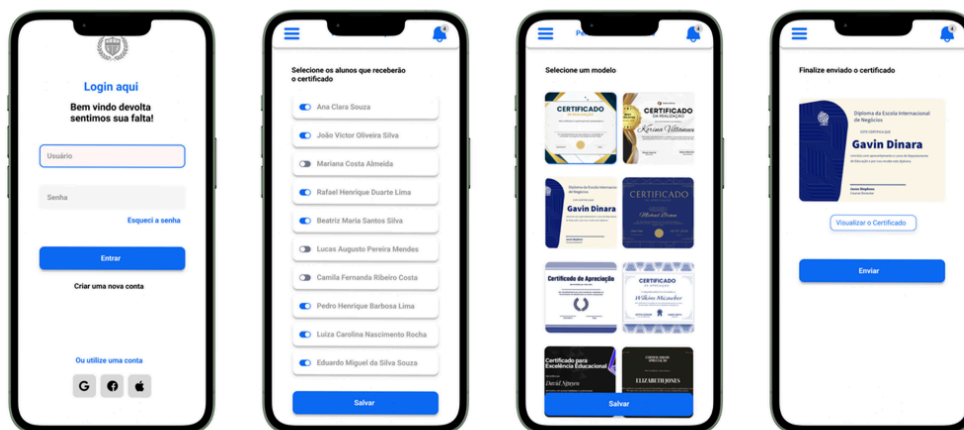


Fonte: Elaborado pelos autores (2025).

As telas projetadas (Figura 6) contemplam o fluxo principal da aplicação, com foco em usabilidade e acessibilidade:

- Login e Autenticação (A): Tela de acesso segura com opções de cadastro e recuperação de senha.
- Perfil e Gerenciamento (B): Menu lateral para o usuário gerenciar seus dados, cadastrar cursos e alunos.
- Personalização e Validação (C): Interface que permite ao usuário escolher modelos, personalizar o certificado e validar os alunos que o receberão.
- Emissão e Confirmação (D): Tela final que exibe uma prévia do documento, permite a emissão e confirma o envio.

Figura 6 - Telas do protótipo de alta fidelidade: (A) Login, (B) Gerenciamento de Conta, (C) Personalização, (D) Emissão e Confirmação.



Fonte: Elaborado pelos autores (2025).

O protótipo foi desenhado com foco em usabilidade e acessibilidade, seguindo as diretrizes do guia de estilo para garantir uma experiência de usuário intuitiva e consistente.

4. CONSIDERAÇÕES FINAIS

O desenvolvimento deste trabalho resultou na criação de um protótipo funcional e bem fundamentado de uma aplicação para a gestão de certificados digitais, que aborda diretamente as lacunas de segurança e usabilidade dos sistemas atuais. A aplicação da metodologia Design Thinking provou ser eficaz, orientando o projeto desde a compreensão das necessidades do usuário até a concepção de uma solução robusta e centrada no ser humano.

A proposta de arquitetura técnica e de segurança detalhada nesta discussão confere ao projeto uma camada de profundidade que vai além da interface, delineando um caminho claro para o desenvolvimento de um sistema completo e confiável. A implementação de assinaturas digitais no padrão PAdES e a estruturação de uma arquitetura segura são diferenciais que posicionam o "Conecte e Certifique" como uma solução alinhada às melhores práticas de segurança da informação (ASSUNÇÃO; SANTOS, 2021).

O protótipo de alta fidelidade desenvolvido atende aos requisitos levantados, oferecendo uma interface intuitiva para funcionalidades como personalização, emissão em múltiplos formatos e gerenciamento de certificados, o que reforça o potencial da solução para otimizar os processos de certificação em contextos educacionais e corporativos.

Como trabalhos futuros, destacam-se três principais frentes:

1. Desenvolvimento e Implementação: Evoluir o protótipo para um Produto Mínimo Viável (MVP), implementando a arquitetura de back-end e front-end proposta.
2. Testes de Usabilidade e Segurança: Realizar testes de usabilidade com usuários reais para refinar a interface e a experiência, bem como testes de penetração (pentest) para validar a eficácia dos mecanismos de segurança implementados.
3. Exploração de Blockchain: Investigar a integração com tecnologia blockchain para o registro dos certificados emitidos. Conforme apontado por Silva et al. *cite_start*, o uso de blockchain pode criar um registro descentralizado, imutável e publicamente verificável, elevando ainda mais o nível de confiabilidade e rastreabilidade dos certificados.

Espera-se que esta solução contribua significativamente para a modernização dos processos de certificação digital, promovendo maior segurança, eficiência e confiança para instituições e usuários.

5. AGRADECIMENTOS

Agradeço primeiramente à minha orientadora, Professora Ivanilse Calderon Ribeiro, pela orientação precisa, paciência, dedicação e por todo o conhecimento compartilhado, que foram essenciais para a condução e o sucesso deste trabalho.

Um agradecimento especial ao Professor Felipe Maia, cujo apoio fundamental e valiosas contribuições foram de imensa importância em todas as etapas deste projeto.

Ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), Campus Porto Velho Zona Norte, pela estrutura e pelo ambiente acadêmico que possibilitaram esta pesquisa.

Aos membros da banca examinadora, Professores Mariela Tamada, Alan Jhone e Tiago Lopes, pela disponibilidade em avaliar este trabalho e pelas pertinentes sugestões que o enriqueceram de forma significativa.

Aos meus colegas de projeto, pela parceria, pelo aprendizado mútuo e pelo trabalho em equipe que tornaram a jornada mais leve e produtiva.

Por fim, dedico este trabalho à minha família e aos meus amigos, por todo o amor, apoio incondicional, compreensão e incentivo que recebi durante todo o percurso.

6. REFERÊNCIAS

ASSUNÇÃO, F.; SANTOS, E. C. Segurança da Informação e Assinaturas Digitais: Fundamentos e Práticas para um Mundo Conectado. São Paulo: Editora Érica, 2021.

BARBOSA, R. Node.js e Express.js: Desenvolvendo Aplicações Web de Alta Performance. Rio de Janeiro: Casa do Código, <https://www.google.com/search?q=2019>.

BROWN, T. Design Thinking. Harvard Business Review, v. 86, n. 6, p. 84-92, 2008.

EL URI, M.; VARGAS, L.; KREUTZ, D. e-certsDS: Certificados eletrônicos com assinatura digital. In: ANAIS ESTENDIDOS DO XXI SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 2021, p. 1-12. SBC.

GOMES, L. A.; ALMEIDA, F. J. Validade Jurídica de Documentos Eletrônicos no Brasil. Curitiba: Juruá Editora, 2022.

ITI. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Padrões de Assinatura Digital ICP-Brasil: DOC-ICP-15 - Versão 10.1. Brasília, DF: ITI, 2021. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/icp-brasil/documentos-icp/docs-icp/doc-icp-15-v-10-1.pdf>. Acesso em: 15 jul. 2025.

MELO, A.; ABELHEIRA, R. Design Thinking & Thinking Design: Metodologia, ferramentas e uma reflexão sobre o tema. São Paulo: Novatec Editora, 2015.

NUNES, J.; QUARESMA, M. A construção de personas e do mapa da jornada do usuário: a delimitação de modelos mentais para o design centrado no usuário ou da interação usuário-notícia. *Estudos em Design*, v. 26, n. 2, p. 3-27, 2018.

OLIVEIRA, P. S. *PostgreSQL: Guia Prático para Administradores de Banco de Dados*. São Paulo: Novatec Editora, 2020.

SILVA, J.; SANTOS, M.; OLIVEIRA, P. Geração e validação de diplomas e certificados utilizando blockchain. In: *ANAIS DO I WORKSHOP EM BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES*, <https://www.google.com/search?q=2019>, p. 13-24. SBC.

SILVA, R. B.; COSTA, A. M. A Modernização dos Processos Acadêmicos: Um Estudo sobre a Emissão de Diplomas Digitais em Universidades Brasileiras. *Revista Brasileira de Informática na Educação*, v. 28, p. 412-430, 2020.

SILVA, T.; LIMA, C. *Desenvolvimento de Aplicações Móveis com Flutter: Teoria e Prática*. Florianópolis: Editora Visual Books, 2021.

VIANNA, M. et al. *Design Thinking: Inovação em Negócios*. Rio de Janeiro: MJV Press, 2012.