INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE – IFRN

MOISÉS ALEXANDRE MONTEIRO ARAUJO

AMBIENTE DIGITAL DE COLETA E ADMINISTRAÇÃO DE ASSINATURAS COLETIVAS

PAU DOS FERROS - RN

2024

MOISÉS ALEXANDRE MONTEIRO ARAUJO

AMBIENTE DIGITAL DE COLETA E ADMINISTRAÇÃO DE ASSINATURAS COLETIVAS

Trabalho de conclusão de curso, apresentado ao curso superior de tecnologia em Análise e Desenvolvimento de Sistemas (TADS) do Instituto Federal de Educação, Ciência e Tecnologia (IFRN) como requisito para a obtenção do título de tecnólogo em análise e desenvolvimento de sistemas.
Orientador: Dr. Thiago Henrique Freire de Oliveira

PAU DOS FERROS - RN

2024

MOISÉS ALEXANDRE MONTEIRO ARAUJO

AMBIENTE DIGITAL DE COLETA E ADMINISTRAÇÃO DE ASSINATURAS COLETIVAS.

Trabalho de conclusão de curso, apresentado ao curso superior de tecnologia em Análise e Desenvolvimento de Sistemas (TADS) do Instituto Federal de Educação, Ciência e Tecnologia (IFRN) como requisito para a obtenção do título de tecnólogo em análise e desenvolvimento de sistemas.
Orientador: Dr. Thiago Henrique Freire de Oliveira

Prof. Dr. Thiago Henrique Freire de Oliveira
Orientador

Prof. Dr. Manoel do Bonfim Lins de Aquino
Examinador Interno

Prof. Dr. Aluísio Igor Rego Fontes
Examinador Interno

PAU DOS FERROS – RN
2024

Araujo, Moisés Alexandre Monteiro.
A837a Ambiente digital de coleta e administração de assinaturas coletivas. / Moisés Alexandre Monteiro Araujo. – 2024.
47 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Pau dos Ferros, 2025.
Orientador (a): Prof. Dr.Thiago Henrique Freire de Oliveira.

1. Assinaturas digitais. 2. Tecnologias modernas. 3. Desenvolvimento de sistema. I. Título.

IFRN/SIbi CDU: 004.4

Sistema Integrado de Bibliotecas
Elaborada pelo Bibliotecário
Rodrigo Mateus Lima Ribeiro – CRB-15/1034

AGRADECIMENTOS

Agradeço, primeiramente, à minha companheira, que esteve ao meu lado durante todo esse tempo, sendo minha maior força e acreditando no meu potencial, mesmo nas circunstâncias mais desafiadoras. Desejo também expressar minha profunda gratidão à minha mãe, que, mesmo à distância, nunca deixou de oferecer seu apoio incondicional. Sua dedicação e palavras de encorajamento foram fundamentais para que eu pudesse superar cada obstáculo ao longo do caminho.

Desejo também expressar minha profunda gratidão à minha mãe, que, apesar da distância, nunca deixou de oferecer seu apoio incondicional. Mesmo de longe, sua dedicação e palavras de encorajamento foram fundamentais para que eu pudesse superar cada obstáculo ao longo do caminho. Deixo meus sinceros agradecimentos ao reitor do curso, Manoel do Bonfim Lins de Aquino, que foi um verdadeiro guia durante minha atuação como monitor. Sua liderança e incentivo foram fundamentais para o meu crescimento acadêmico e pessoal. Agradeço também ao professor Demetrios Araujo Magalhaes Coutinho, pela oportunidade de participar, como voluntário, no Webminário, uma experiencia enriquecedora. Por último, entre os professores mas não menos importante, expresso minha gratidão ao professor e orientador Thiago Henrique Freire de Oliveira, que, durante esta corrida do TCC, não me deixou desistir. Seu apoio constante e incentivo foram fundamentais para que eu pudesse concluir esta etapa com sucesso.

Uma menção especial vai para o universo de ”Elden Ring and Shadows of Erdthree”, cujas terras desoladas e lendas de heróis caídos proporcionaram um refúgio inesperado. Em suas vastas e assombrosas paisagens, encontrei não apenas adversários formidáveis, mas também a força para continuar lutando contra as adversidades deste mundo. Cada batalha travada, cada enigma desvendado, reforçou a coragem e a perseverança necessárias para superar as provas acadêmicas.

Também não posso deixar de agradecer à Crunchyroll, que, nos momentos mais sombrios, nas noites mais solitárias, sob a luz da lua minguante e no silêncio profundo, trouxe vida e cor aos tons cinzas das madrugadas de café e programação. Deixo, assim, meus sinceros agradecimentos a esta ilustre plataforma, que proporcionou alento e inspiração nas horas mais difíceis.

Nota de Respeito: **Bayle the Dread**. A Bayle... o Temido... cuja batalha desafiante nas crateras de Jagged Peak me ensinou a perseverar diante de adversidades mesmo que . Que sua presença imponente e o rigor de seu fogo e relâmpago inspirem coragem a todos que enfrentam seus próprios dragões. Curse you, Bayle!

”People should pursue what they’re passionate about. That will make them happier than pretty much anything else.”
— Elon Musk

ABSTRACT

This project presents the development of a digital platform designed for managing collective signatures, focusing on environments that require multiple signatures, such as meetings, collaborative processes, and formal meeting minutes. The system was designed to centralize signature collection and management in a single digital environment, providing a practical and efficient solution. The platform facilitates signature gathering and data management, allowing the consolidated issuance of signed documents securely and accessibly through a single download. This approach aims to improve the user experience in corporate and academic activities, reducing the time and effort required to complete signing processes while ensuring greater control and security over generated documents.

RESUMO

Este projeto apresenta o desenvolvimento de uma plataforma digital voltada para o gerenciamento de assinaturas coletivas, com foco em ambientes que demandam múltiplas assinaturas, como reuniões, processos colaborativos e atas de encontros formais. O sistema foi projetado para centralizar a coleta e a gestão de assinaturas em um único ambiente digital, proporcionando uma solução prática e eficiente. A plataforma facilita a coleta de assinaturas e o gerenciamento dos dados, permitindo a emissão consolidada de documentos assinados de forma segura e acessível, por meio de um único download. Essa abordagem visa melhorar a experiência dos usuários em atividades corporativas e acadêmicas, reduzindo o tempo e o esforço necessários para completar processos de assinatura, além de garantir maior controle e segurança sobre os documentos gerados.

Palavras-chave: assinaturas digitais, gerenciamento de assinaturas, plataforma digital, eficiência, colaboração.

LISTA DE ILUSTRAÇÕES

Figura 1 – Diagrama de caso de uso do sistema de gerenciamento de assinaturas digitais. Fonte:(MONTEIRO, Moisés, 2024b). 19
Figura 2 – Arquitetura C4-Context, Fonte: (MONTEIRO, Moisés, 2024a). 21
Figura 3 – Tabela do Banco de Dados, Fonte: (MONTEIRO, Moisés, 2024c). 21
Figura 4 – Documentação da *API* com *Django Spectacular* 27
Figura 5 – *ZAP Scanning Report - Development Test* 28
Figura 6 – Fluxograma do Gerenciamento de Assinaturas. Fonte: (MONTEIRO, Moisés, 2024d) 30
Figura 7 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a) 31
Figura 8 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a) 31
Figura 9 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a) 32
Figura 10 – ZAP Scanning Report - expected results 33
Figura 11 – Conclusão Projeto 39

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
DRF	*Django Rest Framework*
MFA	*Multi-Factor Authentication*
HSTS	*HTTP Strict Transport Security*
OWASP ZAP	*Open Web Application Security Project - Zed Attack Proxy*
CSP	*Content Security Policy*
CORS	*Cross-Origin Resource Sharing*
XSS	*Cross-Site Scripting*
CNJ	*Conselho Nacional de Justiça*
MD5	*Message Digest Algorithm 5*
SHA	*Secure Hash Algorithm*
JWKS	*JSON Web Key Set*
JWT	*JSON Web Token*
PBKDF2	*Password-Based Key Derivation Function 2*

SUMÁRIO

1	**INTRODUÇÃO**	**10**
1.1	QUESTÃO DE PESQUISA	11
1.2	OBJETIVOS DO TRABALHO	11
1.3	JUSTIFICATIVA	12
1.4	ORGANIZAÇÃO DO TRABALHO	12
2	**FUNDAMENTAÇÃO TEÓRICA**	**13**
2.1	EVOLUÇÃO HISTÓRICA DAS ASSINATURAS DIGITAIS	13
2.2	ASSINATURAS DIGITAIS, SEGURANÇA JURÍDICA E SEGURANÇA DE DOCUMENTOS	13
2.2.1	**Vulnerabilidades em Algoritmos de *Hash*: Ataques de Colisão**	**14**
2.3	IMPACTO DA PANDEMIA NA ADOÇÃO DE ASSINATURAS DIGITAIS	14
2.4	ABORDAGENS JURÍDICA E TECNOLÓGICA: COMPLEMENTARIDADE	15
2.5	TECNOLOGIA EM MEDIDAS DE SEGURANÇA EM ASSINATURAS DIGITAIS	15
2.5.1	**HTTP (Hypertext Transfer Protocol)**	**15**
2.5.2	**Content Security Policy (CSP)**	**16**
2.5.3	**Strict-Transport-Security (HSTS)**	**16**
2.5.4	**X-Frame-Options**	**16**
2.5.4.1	**Cross-Site Scripting (XSS)**	**17**
2.5.4.2	**Clickjacking**	**17**
3	**METODOLOGIA**	**18**
3.1	METODOLOGIA DE DESENVOLVIMENTO	18
3.2	TECNOLOGIAS UTILIZADAS	19
3.3	ARQUITETURA DO SISTEMA	20
3.4	INTEGRAÇÃO COM API EXTERNA	22
3.5	TESTES DE SEGURANÇA DINÂMICA	22
3.6	COLETA DE DADOS	22
3.7	SEGURANÇA E INTEGRIDADE DOS DADOS	23
3.7.1	**Uso de Algoritmos de Hash**	**23**
3.7.2	**Codificação em Base64**	**23**
3.8	APRIMORAMENTOS E EXPANSÕES PROPOSTAS	24
4	**DESENVOLVIMENTO DO SISTEMA**	**25**
4.1	DESIGN DO SISTEMA	25

4.1.1 Interface do Usuário **25**
4.2 FUNCIONALIDADES IMPLEMENTADAS 26
4.3 INTEGRAÇÃO COM TECNOLOGIAS 26
4.4 DESAFIOS E SOLUÇÕES ADOTADAS 27
4.5 CONSIDERAÇÕES FINAIS SOBRE O DESENVOLVIMENTO 28

5 RESULTADOS ESPERADOS **29**
5.1 EXPECTATIVAS PARA O SISTEMA 29
5.1.1 Funcionalidade Esperada **29**
5.1.2 Usabilidade Esperada **30**
5.1.3 Usabilidade Esperada **30**
5.1.3.1 *Login* **30**
5.1.3.2 Captura de Assinatura **31**
5.1.3.3 Visualização de Dados **32**
5.1.4 Segurança Esperada **32**
5.2 LIMITAÇÕES ESPERADAS 34
5.3 POSSIBILIDADES DE MELHORIAS FUTURAS 34
5.4 CONSIDERAÇÕES FINAIS SOBRE OS RESULTADOS ESPERADOS 34

6 DISCUSSÃO **36**
6.1 COMPARAÇÃO COM SOLUÇÕES EXISTENTES 36
6.2 IMPLICAÇÕES PRÁTICAS 37
6.3 LIMITAÇÕES DO SISTEMA 37
6.4 POSSIBILIDADES DE MELHORIAS FUTURAS 38
6.5 CONSIDERAÇÕES FINAIS 38

7 CONCLUSÃO **39**
7.1 RESUMO DOS PRINCIPAIS RESULTADOS 39
7.2 CONTRIBUIÇÕES DO TRABALHO 39
7.3 LIMITAÇÕES E TRABALHOS FUTUROS 40
7.4 CONSIDERAÇÕES FINAIS 40

Referências **42**

1 INTRODUÇÃO

A implementação de assinaturas digitais tornou-se uma ferramenta fundamental para a autenticação de documentos, sendo então feitos rapidamente, de forma segura e em qualquer lugar, contribuindo para a redução significativa dos custos operacionais(ACRONIS, 2024). Conforme Certinal (CERTINAL, 2024), a digitalização das assinaturas não apenas oferece conveniência, mas é também uma necessidade estratégica para aprimorar a eficiência, minimizar erros e reforçar a segurança da informação. Documentos que exigem múltiplas assinaturas, como atas, exemplificam situações onde um ambiente centralizado de assinaturas digitais pode ser extremamente vantajoso. A gestão manual desses documentos não apenas consome tempo significativo, como também está sujeita a atrasos inesperados, falhas humanas e riscos de segurança que poderiam ser evitados. A digitalização desses processos permite a coleta rápida e organizada de assinaturas, mantendo a integridade e validade legal dos documentos, oferecendo, assim, uma solução eficaz.

A gestão manual desses documentos não só consome um tempo significativo, como também está sujeita a atrasos, falhas humanas e riscos de segurança que poderiam ser evitados. A digitalização desses processos permite a coleta rápida e organizada de assinaturas, mantendo a integridade e validade legal dos documentos. Em termos de viabilidade, essa solução é altamente eficaz para cenários que buscam reduzir a complexidade do processo de assinatura(ACRONIS, 2024).

Por outro lado, embora seja uma solução eficiente para ambientes que necessitam de agilidade e segurança, pode não ser a mais adequada para cenários que requerem um gerenciamento mais robusto de fluxos de trabalho complexos. No entanto, para ambientes acadêmicos e administrativos que lidam com a centralização de um grande volume de assinaturas, essa solução oferece uma forma prática e eficaz de gerenciar múltiplas assinaturas em um único ambiente, garantindo a eficiência e a segurança necessárias para o processo(DRYSIGN, 2024).

Diante desse cenário, este projeto propõe o desenvolvimento de um sistema próprio para o gerenciamento de assinaturas digitais em ambientes acadêmicos e administrativos. Para isso, utilizaremos tecnologias modernas, como o framework Expo(EXPO COMMUNITY, 2024) no desenvolvimento do *front-end* e o *Django REST Framework (DRF)*(DJANGO SOFTWARE FOUNDATION, 2024) no back-end. O objetivo é facilitar a coleta, o armazenamento e o gerenciamento de assinaturas digitais de maneira eficiente e segura, atendendo às demandas específicas desses ambientes.

1.1 QUESTÃO DE PESQUISA

A gestão manual de assinaturas em ambientes acadêmicos e administrativos enfrenta diversos desafios. As ineficiências são comuns: atrasos na coleta de assinaturas, erros durante o processamento, riscos de segurança devido ao manuseio de documentos físicos e dificuldades de acesso para todas as partes envolvidas. Além disso, muitas soluções prontas disponíveis no mercado não oferecem a flexibilidade necessária para personalizar o processo de assinaturas conforme as necessidades específicas de cada instituição. Assim, surge a seguinte questão de pesquisa: ”Como um sistema digital de gerenciamento de assinaturas pode melhorar a eficiência, a segurança e o controle em ambientes acadêmicos e administrativos?”

Essa pergunta busca explorar a viabilidade de um sistema digital de gerenciamento de assinaturas com objetivo de detalhar como a arquitetura de um sistema pode ser estruturada no *front-end* e *back-end*, utilizando tecnologias modernas, como Expo(EXPO COMMUNITY, 2024) e *Django REST Framework (DRF)*(DJANGO SOFTWARE FOUNDATION, 2024), mantendo o foco da pesquisa em criar um ambiente focado na coleta de assinaturas digitais.

1.2 OBJETIVOS DO TRABALHO

O objetivo geral deste trabalho é o desenvolvimento de um sistema que permita a coleta e o gerenciamento de assinaturas digitais, utilizando soluções modernas adequadas às necessidades de ambientes acadêmicos e administrativos. Os objetivos específicos incluem:

- Facilitar a coleta de assinaturas digitais, proporcionando uma interface intuitiva e fácil de usar para os usuários;
- Assegurar que as assinaturas coletadas sejam armazenadas com segurança e ofereçam a flexibilidade necessária para diversas aplicações;
- Permitir que os usuários visualizem as assinaturas de maneira restrita, garantindo privacidade e controle de acesso adequado;
- Fornecer aos administradores a capacidade de gerenciar todas as assinaturas e extrair dados para análises posteriores, promovendo a tomada de decisões informadas; e
- Implementar o sistema utilizando Expo(EXPO COMMUNITY, 2024) para o *front-end* e *Django REST Framework (DRF)*(DJANGO SOFTWARE FOUNDATION, 2024) para o *back-end*, explorando ao máximo as vantagens dessas tecnologias, como a capacidade de desenvolvimento ágil e a robustez na gestão de APIs.

1.3 JUSTIFICATIVA

A decisão de desenvolver um sistema próprio para o gerenciamento de assinaturas digitais é justificada pela necessidade crescente de modernizar os processos administrativos e acadêmicos de forma eficiente e personalizada. Soluções prontas no mercado muitas vezes não oferecem a flexibilidade desejada para atender às demandas específicas das instituições. Ao desenvolver um sistema internamente, é possível realizar adaptações conforme as necessidades exatas da instituição, garantindo maior controle e segurança. Além disso, a escolha de tecnologias como o Expo(EXPO COMMUNITY, 2024) e o *Django REST Framework (DRF)*(DJANGO SOFTWARE FOUNDATION, 2024) permite o desenvolvimento de uma aplicação multiplataforma ágil, melhorando a acessibilidade e a usabilidade para todos os usuários.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado da seguinte forma:

- O **Capítulo 2** traz a **Fundamentação Teórica**, discutindo a evolução histórica das assinaturas digitais, com base na pesquisa de Elysa Freitas (2021)(MELO, 2021), os mecanismos de segurança associados, o impacto da pandemia na adoção dessas tecnologias, e a complementação entre abordagens jurídicas e tecnológicas.
- O **Capítulo 3** descreve a **metodologia** adotada para o desenvolvimento do sistema, incluindo a abordagem ágil utilizada e as tecnologias envolvidas.
- O **Capítulo 4** detalha o processo de **desenvolvimento** do sistema, apresentando o design da aplicação, as funcionalidades implementadas e a integração com APIs.
- O **Capítulo 5** mostra os **resultados esperados** obtidos com a implementação do sistema, destacando as vantagens alcançadas e as limitações encontradas.
- O **Capítulo 6** traz a **discussão** dos resultados, comparando o sistema desenvolvido com outras soluções existentes no mercado e avalia o impacto de suas características diferenciadoras.
- O **Capítulo 7** traz a **conclusão** do trabalho, sintetizando os principais pontos discutidos, as contribuições realizadas, e sugerindo possíveis direções para pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 EVOLUÇÃO HISTÓRICA DAS ASSINATURAS DIGITAIS

A evolução das assinaturas digitais está intimamente ligada ao desenvolvimento das formas de autenticação e segurança dos documentos ao longo da história. Desde a antiguidade, as sociedades buscaram formas mais seguras de formalizar acordos, passando dos contratos verbais para os escritos, à medida que as relações sociais e econômicas se tornaram mais complexas (MELO, 2021). No Brasil, isso culminou na criação de mecanismos de validação de documentos em cartórios, com o reconhecimento de firma sendo uma prática comum para assegurar a autenticidade e validade jurídica dos documentos físicos (MELO, 2021).

Antes da adoção das assinaturas eletrônicas nos cartórios, o reconhecimento de firma era um processo manual e presencial. O cidadão precisava comparecer fisicamente ao cartório para assinar o documento ou confirmar sua assinatura. O tabelião comparava a nova assinatura com as que estavam arquivadas em uma ficha de firma previamente registrada. Esse procedimento, apesar de assegurar a autenticidade, era lento e suscetível a erros humanos (BRASIL, C. N. do, 2020; NAVIGANDI, 2020).

Com o avanço da tecnologia, especialmente a partir de 2001, a Medida Provisória 2.200-2 estabeleceu a Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), possibilitando a emissão de certificados digitais para assinatura de documentos eletrônicos. No entanto, a pandemia de COVID-19 acelerou ainda mais a adoção de assinaturas digitais. O Provimento nº 100/2020 do CNJ permitiu a realização de atos notariais eletrônicos, marcando uma transformação significativa no processo de autenticação documental (JUSTIÇA (CNJ), 2020; IGREE, 2020).

Esses avanços permitiram a utilização de assinaturas digitais e o reconhecimento de firma online, trazendo agilidade e segurança ao processo (E-NOTARIADO, s.d.).

2.2 ASSINATURAS DIGITAIS, SEGURANÇA JURÍDICA E SEGURANÇA DE DOCUMENTOS

As assinaturas digitais são uma inovação importante em termos de segurança jurídica e eficiência na autenticação de documentos eletrônicos. A base dessa tecnologia é a criptografia, que garante a autenticidade e integridade dos documentos, evitando fraudes (BRASIL, s.d.; DONIZETTI, 2020).

A criptografia assimétrica, utilizada nas assinaturas digitais, faz uso de dois ti-

pos de chaves: uma pública e uma privada. Enquanto o detentor da chave privada assina o documento, a chave pública permite verificar sua autenticidade (DONIZETTI, 2020). Apesar de sua robustez, desafios como o custo elevado dos certificados digitais e vulnerabilidades tecnológicas ainda persistem (MELO, 2021). Para garantir a integridade dos documentos, algoritmos de criptografia são amplamente empregados. Assim, qualquer alteração no conteúdo de um documento é facilmente detectada (SANTOS MACHADO, 2020).

2.2.1 Vulnerabilidades em Algoritmos de *Hash*: Ataques de Colisão

Os algoritmos de *hash* são utilizados para garantir a integridade dos dados, gerando um código único para cada conjunto de informações. No entanto, ataques de colisão — quando dois conjuntos de dados diferentes produzem o mesmo valor de *hash* — comprometem a segurança do sistema.

O *MD5*, amplamente utilizado no passado, tornou-se vulnerável a esses ataques, sendo inadequado para aplicações que exigem alta segurança (RIVEST, 1992). Da mesma forma, o *SHA-1* foi considerado inseguro após a descoberta de colisões geradas de maneira eficiente (SCHNEIER, 1996). Em resposta a essas vulnerabilidades, algoritmos mais robustos, como o *SHA-256*, foram adotados, oferecendo uma proteção maior contra ataques de colisão (KRAWCZYK; BELLARE; CANETTI, 1995; STANDARDS; TECHNOLOGY, 2015).

Atualmente, o *SHA-256* é amplamente utilizado em sistemas de segurança e autenticação, como no *Django Rest Framework*, empregado neste trabalho para garantir a integridade dos dados (DJANGO SOFTWARE FOUNDATION, 2024).

2.3 IMPACTO DA PANDEMIA NA ADOÇÃO DE ASSINATURAS DIGITAIS

A pandemia de COVID-19 acelerou significativamente a adoção de tecnologias digitais em diversos setores. Durante o período de isolamento social, a validação de documentos de forma remota tornou-se essencial para a continuidade das operações administrativas e jurídicas (SILVA, 2021). O Provimento nº 100/2020 do Conselho Nacional de Justiça (CNJ) permitiu a realização de atos notariais eletrônicos, consolidando o uso de assinaturas digitais no Brasil (JUSTIÇA (CNJ), 2020).

A adaptação rápida de empresas e órgãos públicos para garantir a continuidade de suas operações foi um marco importante na modernização dos processos burocráticos, eliminando a necessidade de presença física e reduzindo a burocracia envolvida nos procedimentos tradicionais (MELO, 2021).

2.4 ABORDAGENS JURÍDICA E TECNOLÓGICA: COMPLEMENTARIDADE

Este trabalho concentra-se na implementação prática de plataformas de assinaturas digitais. No entanto, a aceitação dessas tecnologias no âmbito legal depende de adaptações regulatórias. A Lei 14.063/2020 foi um marco ao integrar as assinaturas digitais no setor público e privado, estabelecendo diferentes níveis de assinatura digital, cada um com seu grau de confiabilidade (BRASIL, s.d.; DONIZETTI, 2020).

2.5 TECNOLOGIA EM MEDIDAS DE SEGURANÇA EM ASSINATURAS DIGITAIS

Com o crescimento acelerado no uso de assinaturas digitais em sistemas online, impulsionado pela digitalização e pela pandemia de *COVID-19*, a proteção contra ameaças cibernéticas tornou-se fundamental para garantir a integridade dos dados e a segurança dos usuários. Segundo relatórios, o mercado de assinaturas digitais cresceu de US$ 1,83 bilhão em 2019 para um valor estimado de US$ 4,95 bilhões em 2023, com uma taxa de crescimento anual de 27,69% (GUNAWAN et al., 2022). Além disso, a *OWASPZAP*(FOUNDATION, O., 2024) indica que o *Cross-Site Scripting (XSS)* é uma das vulnerabilidades mais comuns em aplicações *web*, permitindo que atacantes injetem scripts maliciosos em páginas visualizadas por outros usuários, comprometendo a segurança dos dados e possibilitando o roubo de informações sensíveis, como cookies de sessão (HOSTING, 2024). Já o *Clickjacking* é uma técnica em que os usuários são enganados para clicar em algo diferente do que percebem, o que pode resultar na execução de ações não autorizadas, como a modificação ou aprovação indevida de documentos assinados digitalmente (INC., S., 2024) (LLC, I., 2024).

2.5.1 HTTP (Hypertext Transfer Protocol)

O *HTTP* (Hypertext Transfer Protocol) é o protocolo fundamental utilizado para a comunicação entre clientes (navegadores) e servidores na *web*. Ele é responsável por definir como as mensagens são formatadas e transmitidas, além de determinar as ações que os servidores e navegadores devem realizar em resposta a diferentes comandos. Originalmente, o *HTTP* foi desenvolvido como um protocolo de texto simples, o que o torna vulnerável a ataques como a interceptação de dados (*Man-in-the-Middle*) e a modificação não autorizada de informações durante a comunicação ((IETF), 2014).

Para resolver essas vulnerabilidades, surgiu o *HTTPS* (*HTTP Secure*), que adiciona uma camada de criptografia através do protocolo *SSL/TLS* (*Secure Sockets Layer/Transport Layer Security*). Isso garante que os dados transmitidos entre o cliente e o servidor sejam protegidos contra interceptações e modificações.

2.5.2 Content Security Policy (CSP)

O *Content Security Policy* (CSP) é uma política de segurança projetada para mitigar e prevenir certos tipos de ataques, como *Cross-Site Scripting* (XSS) e injeção de dados, que podem comprometer a segurança de uma aplicação *web*. Ele funciona permitindo que os desenvolvedores especifiquem de quais fontes o navegador pode carregar conteúdo (scripts, estilos, imagens, etc.), bloqueando a execução de scripts não autorizados.

Essa política é considerada uma das defesas mais robustas contra ataques *XSS*, pois impede que scripts maliciosos sejam carregados e executados no navegador dos usuários (W3C, 2021). O *CSP* pode ser implementado através de um cabeçalho *HTTP* específico, o *Content-Security-Policy*, que é enviado junto às respostas do servidor.

2.5.3 Strict-Transport-Security (HSTS)

O Strict-Transport-Security (HSTS) é uma política de segurança que protege os usuários contra ataques de interceptação, como o ataque Man-in-the-Middle (MITM). Quando um servidor implementa HSTS, ele informa aos navegadores que apenas conexões seguras via HTTPS devem ser utilizadas para se comunicar com o servidor. Isso impede que navegadores façam conexões não seguras (HTTP), mesmo se o usuário tentar acessar a URL sem o prefixo ”https”.

A principal vantagem do HSTS é garantir que a comunicação entre cliente e servidor seja sempre criptografada, aumentando a segurança das informações trocadas durante a navegação ((IETF), 2012).

2.5.4 X-Frame-Options

O cabeçalho X-Frame-Options é outra medida de segurança importante utilizada para prevenir ataques de Clickjacking. O Clickjacking ocorre quando uma página maliciosa incorpora outra página legítima em um iframe, escondendo o conteúdo e induzindo o usuário a realizar ações não intencionadas, como aprovar uma transação ou clicar em um botão oculto.

A implementação do cabeçalho X-Frame-Options impede que uma página seja carregada em iframes de domínios não autorizados, protegendo o sistema contra esses tipos de ataques. O cabeçalho pode ser configurado com valores como DENY (impede completamente o carregamento em iframes) ou SAMEORIGIN (permite o carregamento em iframes somente se forem do mesmo domínio) ((IETF), 2010).

2.5.4.1 Cross-Site Scripting (XSS)

O *Cross-Site Scripting* (XSS) é uma vulnerabilidade que permite que scripts maliciosos sejam injetados em páginas da *web*, sendo executados pelos navegadores dos usuários que acessam essas páginas. Em um sistema de assinaturas digitais, essa falha pode ser explorada para roubar informações confidenciais, como credenciais de usuários, ou alterar a funcionalidade do sistema sem autorização, colocando em risco a integridade dos documentos assinados.

Para mitigar esse tipo de ataque, a implementação do cabeçalho *Content Security Policy* (CSP) é uma medida eficaz. O *CSP* restringe as fontes de conteúdo que podem ser carregadas na página, bloqueando scripts não autorizados e prevenindo a execução de códigos maliciosos. Segundo a OWASP, o *CSP* é uma das defesas mais robustas contra ataques *XSS* (FOUNDATION, O., 2024).

2.5.4.2 Clickjacking

O *Clickjacking* é um ataque em que o usuário é induzido a clicar em algo diferente do que ele pensa estar clicando. Isso é feito através do uso de *iframes* invisíveis ou disfarçados, que sobrepõem a página legítima, permitindo que o invasor capture as ações do usuário, como aprovar assinaturas ou executar comandos sem seu consentimento.

Para prevenir ataques de *Clickjacking* em um sistema de assinaturas digitais, é recomendado o uso do cabeçalho *X-Frame-Options*, que impede que a página seja carregada dentro de um *iframe* não autorizado. Essa medida assegura que a aplicação só possa ser exibida diretamente, prevenindo tentativas de enganar o usuário e protegendo a integridade das ações realizadas dentro do sistema (FOUNDATION, O., 2024).

3 METODOLOGIA

Este capítulo descreve a metodologia adotada para o desenvolvimento do sistema de gerenciamento de assinaturas digitais, destacando as abordagens e processos utilizados. O objetivo é apresentar de forma clara as etapas do desenvolvimento, desde a escolha das tecnologias até a implementação e integração das soluções. Nos subcapítulos seguintes, são detalhadas as ferramentas e APIs empregadas, como o uso de autenticação segura e assinaturas digitais, além das decisões tomadas para garantir a segurança e a eficiência do sistema.

Nos tópicos a seguir, serão abordados:

- A escolha das tecnologias, incluindo a utilização de APIs externas, como a API *Clerk*(INC., C., 2024), para autenticação segura com *Google*(LLC, G., 2024), e a integração dessas tecnologias ao sistema.
- O processo de desenvolvimento adotado, enfatizando as boas práticas de segurança e os algoritmos de hash aplicados.
- A arquitetura do sistema e as decisões técnicas que visam garantir a escalabilidade e integridade dos dados.

Essas seções detalharão os materiais e as ferramentas escolhidas, além de discutir os princípios metodológicos que guiaram o desenvolvimento do sistema de gerenciamento de assinaturas digitais.

3.1 METODOLOGIA DE DESENVOLVIMENTO

O desenvolvimento do sistema foi conduzido de forma independente, adotando uma abordagem ágil adaptada para trabalho individual. As etapas incluíram:

- Planejamento incremental: Divisão do desenvolvimento em pequenas etapas com objetivos específicos e entregas constantes.
- Revisão contínua: Avaliação contínua do progresso, ajustes de prioridades e implementação de melhorias conforme necessário.
- Adaptação rápida: Flexibilidade para modificar funcionalidades com base em testes e feedback de usuários, promovendo a melhoria contínua, logo visto abaixo na Figura 1.

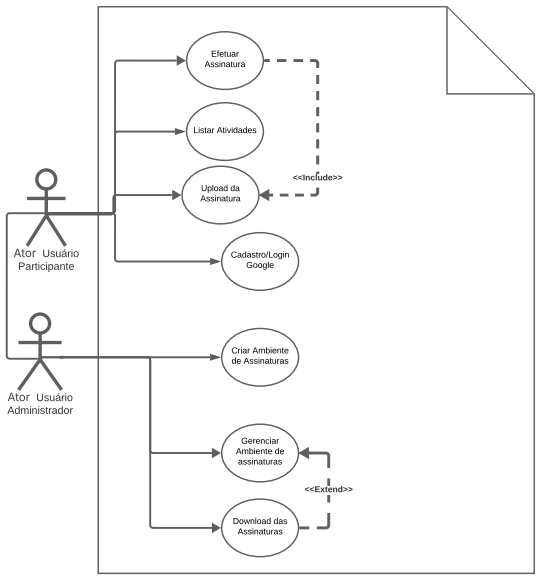


Figura 1 – Diagrama de caso de uso do sistema de gerenciamento de assinaturas digitais. Fonte:(MONTEIRO, Moisés, 2024b).

3.2 TECNOLOGIAS UTILIZADAS

O sistema foi desenvolvido para combinar o uso de tecnologias modernas e garantir desempenho, segurança e escalabilidade:

- *Expo* (*front-end*): Utilizado para a interface do usuário, garantindo uma experiência responsiva e intuitiva. Atualmente funcional apenas na web, com possibilidade de expansão para dispositivos móveis no futuro.
- *Django REST Framework*k(DJANGO SOFTWARE FOUNDATION, 2024) (DRF) (*back-end*): Usado para a criação de APIs RESTful, o que permite integração segura e escalável com o *front-end*.
- *Clerk*(INC., C., 2024): Implementado como serviço de autenticação externa, realizando login com *Google*(LLC, G., 2024). A escolha pelo *Clerk* foi baseada em sua facilidade de uso, integração simples com *React Native*(META PLATFORMS, INC., 2024) e nas ferramentas gratuitas oferecidas na versão limitada. Além

disso, o *Clerk* oferece um alto nível de segurança, utilizando criptografia forte, como o algoritmo **AES** (Advanced Encryption Standard) para proteger dados sensíveis, e o algoritmo de **hash bcrypt** para a proteção de senhas, garantindo segurança no armazenamento e gerenciamento dos dados dos usuários(PROVOS; MAZIÈRES, 1999; DAEMEN; RIJMEN, 2001; CLERK, 2024).

- Bibliotecas complementares: Utilização de *React Native View Shot*(GREATH APES, INC., 2024) para captura de assinaturas e Axios para comunicação entre cliente e servidor.

3.3 ARQUITETURA DO SISTEMA

A arquitetura adotada é do tipo cliente-servidor, com componentes distintos para garantir modularidade e segurança:

- Camada de apresentação (*front-end*): Desenvolvida com Expo para captura e exibição de assinaturas, gerenciamento de informações de usuários e integração com a API *Clerk*(INC., C., 2024) para autenticação segura com *Google*(LLC, G., 2024).

- camada de lógica de negócio (*back-end*): Implementada com *Django REST Framework*(DJANGO SOFTWARE FOUNDATION, 2024) (DRF) (*back-end*), gerencia autenticação, validação de dados e controle de acesso, e se comunica com o *Clerk*(INC., C., 2024) para validação de tokens de usuário, logo a baixo estará exemplificado como é base em Arquitetura de Contexto na Figura 2.

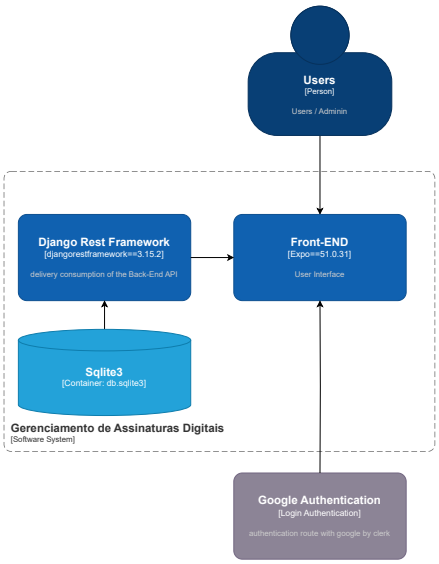


Figura 2 – Arquitetura C4-Context, Fonte: (MONTEIRO, Moisés, 2024a).

- Camada de persistência de dados: Utiliza um banco de dados relacional para armazenar dados de usuários, assinaturas e referências de autenticação, com exemplo detalhado de sua tabela na Figura 3 a baixo.

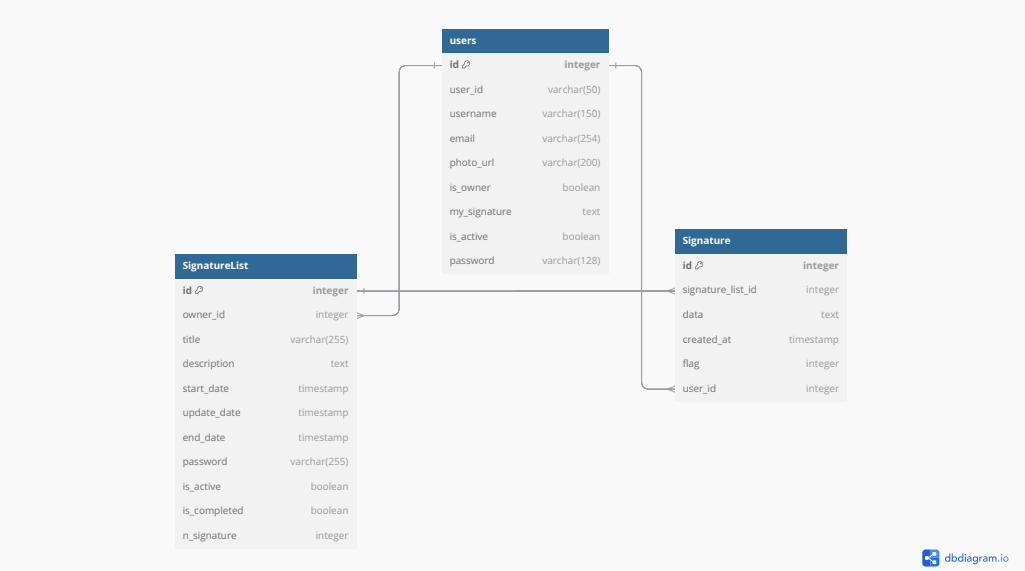


Figura 3 – Tabela do Banco de Dados, Fonte: (MONTEIRO, Moisés, 2024c).

3.4 INTEGRAÇÃO COM API EXTERNA

Para o gerenciamento da autenticação de usuários, foi integrada a API que permite o login com *Google*(LLC, G., 2024) de maneira segura. A implementação envolveu:

- Configuração inicial: Registro do projeto no *Clerk*(INC., C., 2024) e obtenção das credenciais de API.
- Integração no *front-end*: Uso dos componentes do *Clerk*(INC., C., 2024) para adicionar a funcionalidade de login com *Google*(LLC, G., 2024) diretamente na interface do usuário, garantindo uma experiência de login segura e sem fricções.
- Verificação no *back-end*: O servidor com *Django*(DJANGO SOFTWARE FOUNDATION, 2024) usa os tokens de autenticação gerados pelo *Clerk*(INC., C., 2024) para validar sessões e autorizar acesso a recursos protegidos, utilizando métodos avançados de verificação de identidade para garantir a segurança.

3.5 TESTES DE SEGURANÇA DINÂMICA

Para garantir a robustez e a segurança do sistema de gerenciamento de assinaturas digitais, foram realizados testes de segurança dinâmica utilizando a ferramenta OWASP ZAP(FOUNDATION, O., 2024) (Zed Attack Proxy). Este teste foi configurado para ser executado automaticamente através do GitHub Actions, permitindo a detecção contínua de vulnerabilidades de segurança na aplicação web.

O OWASP ZAP(FOUNDATION, O., 2024) foi escolhido por ser uma ferramenta de código aberto amplamente utilizada para testes de segurança em aplicações web. É capaz de identificar vulnerabilidades como injeções SQL, exposição de informações sensíveis, cross-site scripting (XSS), entre outras.

Como o projeto estava em um ambiente de desenvolvimento local, foi utilizada a versão gratuita do Ngrok(LLC, N., 2024) para expor temporariamente a aplicação web em uma porta específica durante a execução dos testes, permitindo que o OWASP ZAP(FOUNDATION, O., 2024) realizasse a análise de segurança necessária.

3.6 COLETA DE DADOS

A coleta de dados é realizada principalmente através da integração da API externa para autenticação de usuários. O sistema captura as informações necessárias para o gerenciamento de assinaturas digitais de forma segura e eficiente.

- Integração com *Clerk*(INC., C., 2024): Utilização de componentes do *Clerk*(INC., C., 2024) para permitir login seguro com *Google*(LLC, G., 2024) diretamente na interface do usuário, garantindo uma experiência fluida.
- Armazenamento de Dados: Os dados capturados, como informações de usuários e assinaturas, são armazenados em um banco de dados relacional, mantendo a integridade.

3.7 SEGURANÇA E INTEGRIDADE DOS DADOS

Para garantir a segurança e a integridade dos dados, o sistema utiliza algoritmos de *hash* e a codificação *Base64*. Essas técnicas asseguram que os dados armazenados e transmitidos não sofram alterações indevidas e possam ser validados de maneira eficiente.

3.7.1 Uso de Algoritmos de Hash

Os algoritmos de *hash* são amplamente utilizados para verificar a integridade dos dados no sistema. O *SHA-256* foi escolhido como o algoritmo de *hash* principal devido à sua alta resistência a ataques de colisão e sua confiabilidade em ambientes que exigem alta segurança (KRAWCZYK; BELLARE; CANETTI, 1995; STANDARDS; TECHNOLOGY, 2015). Este algoritmo gera um código único para cada documento ou assinatura, permitindo que qualquer modificação no conteúdo seja facilmente detectada. Ao gerar e armazenar os *hashes* de documentos assinados digitalmente, o sistema é capaz de garantir que os dados não sejam alterados durante a transmissão ou armazenamento.

3.7.2 Codificação em Base64

Além do uso de *hash*, o sistema emprega a codificação *Base64* para armazenar e transmitir dados de maneira eficiente e compatível com diferentes plataformas. A codificação *Base64* converte dados binários em strings de caracteres ASCII, o que facilita o armazenamento em bancos de dados e a transmissão através de APIs RESTful. Isso é particularmente útil ao lidar com assinaturas digitais e outros dados binários que precisam ser armazenados ou transmitidos como texto.

Os principais benefícios do *Base64* incluem:

- **Compatibilidade com diversos sistemas**: A codificação *Base64* é amplamente utilizada para permitir que dados binários, como imagens ou assinaturas digitais, sejam armazenados e transmitidos por sistemas que lidam com texto, como bancos de dados e APIs RESTful (**base64_standard**).

- **Transmissão mais estável**: Embora o *Base64* não seja um mecanismo de criptografia, ele ajuda a evitar problemas de transmissão de dados binários em sistemas que só processam texto, minimizando o risco de perda de dados ou corrupção durante o envio (JOSEFSSON, 2006).
- **Facilidade de integração**: O *Base64* facilita a integração entre diferentes sistemas, pois converte dados binários em strings ASCII, o que simplifica a compatibilidade com várias linguagens de programação e padrões de comunicação (MCGREW, 2018).

Embora a codificação *Base64* aumente o tamanho dos dados em cerca de 33%, a sua capacidade de garantir uma transmissão segura e compatível com diversos sistemas compensa esse aumento (JOSEFSSON, 2006). No sistema desenvolvido, *Base64* é utilizado para transmitir e armazenar dados como assinaturas digitais e certificados, garantindo compatibilidade e integridade em todas as fases do processo.

3.8 APRIMORAMENTOS E EXPANSÕES PROPOSTAS

A metodologia adotada inclui planos para expandir a aplicação para dispositivos móveis, adicionar funcionalidades conforme as necessidades dos usuários, e aprimorar a integração ao *Clerk*(INC., C., 2024) para suportar novos métodos de autenticação, mantendo um alto nível de segurança.

4 DESENVOLVIMENTO DO SISTEMA

O processo de desenvolvimento do sistema de gerenciamento de assinaturas digitais destaca as decisões de design, a implementação das funcionalidades principais e a integração com as tecnologias utilizadas. O sistema foi desenvolvido com foco em ambiente web, mantendo a flexibilidade para futuras expansões para dispositivos móveis.

4.1 DESIGN DO SISTEMA

O design do sistema foi guiado pela necessidade de criar uma interface amigável e intuitiva, proporcionando uma experiência de usuário eficiente e sem complicações. A interface foi desenvolvida utilizando o Expo (EXPO COMMUNITY, 2024) para web, visando uma navegação simplificada e responsiva, que facilita a captura de assinaturas digitais de maneira prática e segura.

4.1.1 Interface do Usuário

A interface do usuário foi criada com componentes do *React Native*(META PLATFORMS, INC., 2024) e Expo(EXPO COMMUNITY, 2024) , com ênfase em simplicidade e usabilidade. O design priorizou o fácil acesso às funcionalidades principais, assegurando que os usuários possam gerenciar suas assinaturas e informações de forma intuitiva. As funcionalidades implementadas na interface incluem:

- **Formulários de cadastro e login**: Interfaces para registro e autenticação de usuários, integradas com a API do back-end e utilizando o *Clerk*(INC., C., 2024) para autenticação via Google(LLC, G., 2024), garantindo segurança e praticidade.
- **Captura de assinaturas digitais**: Implementada com a biblioteca *react-native-view-shot*, permite que os usuários assinem documentos diretamente na tela. As assinaturas são enviadas do front-end para o back-end através da API, para armazenamento seguro no servidor.
- **Gestão de assinaturas**: Funcionalidade que permite aos usuários visualizar suas próprias assinaturas e as informações do responsável pela coleta, como nome, e-mail e foto, promovendo confiança entre os usuários.
- **Configuração de privacidade e acesso**: Opções para que o administrador crie senhas e defina níveis de acesso, assegurando a privacidade nos ambientes de listagem das assinaturas.

4.2 FUNCIONALIDADES IMPLEMENTADAS

O desenvolvimento do sistema focou na implementação das seguintes funcionalidades principais:

- **Cadastro e autenticação de usuários**: Utilizando o Django REST Framework(DJANGO SOFTWARE FOUNDATION, 2024), foi criada uma API para gerenciar o cadastro e login de usuários. A autenticação é feita por meio de tokens, integrados com o *Clerk*(INC., C., 2024), garantindo que apenas usuários autenticados possam acessar o sistema de maneira segura.
- **Envio e Armazenamento de assinaturas digitais**: A captura de assinaturas, implementada com *react-native-view-shot*, permite que os usuários assinem documentos diretamente na interface web. As assinaturas são enviadas para o servidor usando Axios e armazenadas no banco de dados, seguindo padrões de segurança.
- **Visualização restrita de assinaturas**: O sistema permite que os usuários visualizem assinaturas e informações relacionadas de forma restrita, protegendo a privacidade e promovendo transparência na troca de informações.
- **Exportação de dados e assinaturas**: O administrador pode extrair dados coletados para análises futuras ou para integração com outros sistemas, oferecendo flexibilidade no uso das assinaturas digitais.

4.3 INTEGRAÇÃO COM TECNOLOGIAS

A integração entre o front-end e o back-end foi realizada utilizando APIs RESTful, com o *Django REST Framework (DRF)*(DJANGO SOFTWARE FOUNDATION, 2024) no servidor e Expo(EXPO COMMUNITY, 2024) no cliente. As principais bibliotecas e ferramentas utilizadas incluem:

- ***React Native*(META PLATFORMS, INC., 2024) e Expo(EXPO COMMUNITY, 2024)** : Utilizados para desenvolver a interface do usuário e permitir a captura de assinaturas digitais.
- ***Django REST Framework (DRF)***(DJANGO SOFTWARE FOUNDATION, 2024) : Responsável pela lógica de negócio e gerenciamento de dados no servidor. A API criada com DRF possibilita a comunicação segura e eficiente entre cliente e servidor.
- **Axios**: Biblioteca de requisições HTTP popularmente utilizada no front-end para enviar dados capturados, como assinaturas, para a API do servidor.

- **React-native-view-shot**(GREATH APES, INC., 2024): Utilizada para capturar assinaturas digitais diretamente da tela do usuário, que são enviadas para o servidor.
- ***Clerk*(INC., C., 2024) (Autenticação com Google(LLC, G., 2024))**: Utilizado para autenticação segura de usuários, proporcionando uma integração simples com métodos de login populares e oferecendo recursos avançados de segurança e privacidade.

4.4 DESAFIOS E SOLUÇÕES ADOTADAS

Durante o desenvolvimento do sistema, diversos desafios foram enfrentados, especialmente em relação à captura e armazenamento de assinaturas digitais, segurança e controle de acesso. As soluções adotadas incluem:

- **Documentação da *API* com *Django Spectacular***: Para melhorar a documentação da *API* e facilitar o desenvolvimento, foi usado o *Django Spectacular*, que gera documentação em conformidade com o *OpenAPI 3.0*. A documentação da *API*, intitulada ***Signatures List Api 1.0.0***, abrange todos os *endpoints* disponíveis no sistema, incluindo operações relacionadas a listas de assinaturas e assinaturas individuais, autenticação de usuários e gerenciamento de dados. A Figura 4 abaixo ilustra os principais endpoints documentados.

Figura 4 – Documentação da *API* com *Django Spectacular*

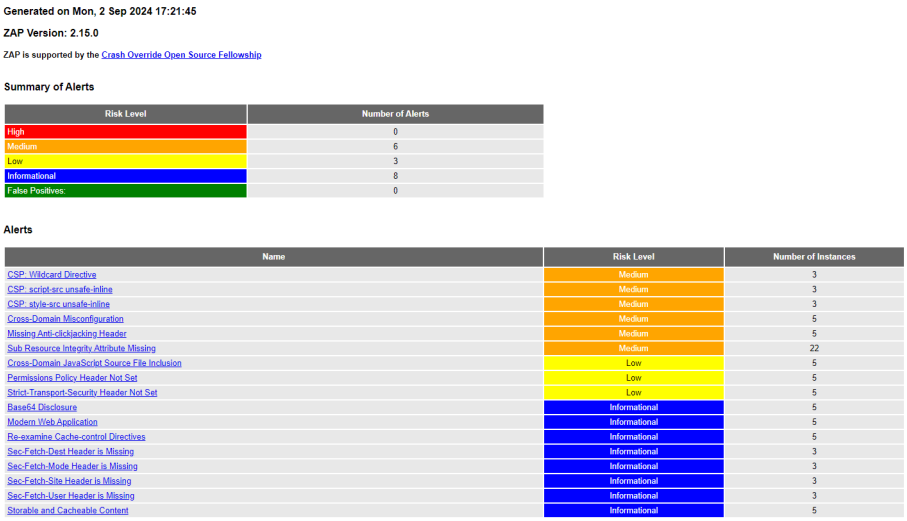
Fonte: (AL., 2024)(DJANGO SOFTWARE FOUNDATION, 2024)

Captura e armazenamento: A escolha da biblioteca *react-native-view-shot*(GREATH APES, INC., 2024) permitiu capturar assinaturas de maneira eficiente. Ajustes foram

feitos para otimizar a compatibilidade com diferentes formatos de assinatura, como nome completo ou rubrica.

segurança de acesso: A autenticação baseada em *tokens* foi implementada usando o *Django Auth Token*(FOUNDATION, D. S., 2024), junto com uso do *Clerk*(INC., C., 2024) para login com *Google*(LLC, G., 2024), garantiu que somente os usuários que são autorizados podem ter acesso a informações sensíveis. Esta abordagem permite configurar níveis de privacidade para documentos e assinaturas, oferecendo mais segurança e controle para acessar dados.

Durante o desenvolvimento, foi detectado um número maior de alertas de segurança devido à configuração permissiva ‘[’*’]‘ no arquivo ‘settings‘. Após ajustes, como a inclusão da *Content Security Policy (CSP)*, o número de vulnerabilidades foi significativamente reduzido. Na Figura 5, apresenta-se um exemplo do teste realizado ao longo do desenvolvimento, conduzido com a ferramenta *OWASP ZAP*(FOUNDATION, O., 2024).



Generated on Mon, 2 Sep 2024 17:21:45

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	3
Informational	8
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	3
CSP: script-src unsafe-inline	Medium	3
CSP: style-src unsafe-inline	Medium	3
Cross-Domain Misconfiguration	Medium	5
Missing Anti-clickjacking Header	Medium	5
Sub Resource Integrity Attribute Missing	Medium	22
Cross-Domain JavaScript Source File Inclusion	Low	5
Permissions Policy Header Not Set	Low	5
Strict-Transport-Security Header Not Set	Low	5
Base64 Disclosure	Informational	5
Modern Web Application	Informational	5
Re-examine Cache-control Directives	Informational	5
Sec-Fetch-Dest Header is Missing	Informational	3
Sec-Fetch-Mode Header is Missing	Informational	3
Sec-Fetch-Site Header is Missing	Informational	3
Sec-Fetch-User Header is Missing	Informational	3
Storable and Cacheable Content	Informational	5

Figura 5 – *ZAP Scanning Report - Development Test*

Fonte: (FOUNDATION, O., 2024)(LLC, N., 2024)

4.5 CONSIDERAÇÕES FINAIS SOBRE O DESENVOLVIMENTO

O desenvolvimento do sistema inicialmente focou no ambiente *web*, demonstrando ser uma base sólida para expansões futuras para outras plataformas, como dispositivos móveis. A escolha das tecnologias e ferramentas usadas permitiu uma implementação eficiente, com potencial **flexibilidade** para atender a diversas necessidades dos usuários.

5 RESULTADOS ESPERADOS

Este capítulo apresenta os resultados esperados do sistema de gerenciamento de assinaturas digitais, baseados em sua funcionalidade, usabilidade, segurança e desempenho. O objetivo é delinear as principais vantagens e limitações que se espera que o sistema apresente após sua implementação e testes adequados.

5.1 EXPECTATIVAS PARA O SISTEMA

Com base no desenvolvimento inicial, espera-se que o sistema seja capaz de gerenciar assinaturas digitais de maneira eficiente, atendendo aos objetivos propostos. As expectativas para o sistema são abordadas em diferentes aspectos:

5.1.1 Funcionalidade Esperada

Espera-se que o sistema capture e armazene assinaturas digitais de forma eficaz, utilizando a biblioteca *react-native-view-shot*(GREATH APES, INC., 2024) para capturar assinaturas diretamente na interface da web. A comunicação entre o *front-end* e o *back-end*, via *APIs RESTful*(DJANGO SOFTWARE FOUNDATION, 2024), deve permitir o **envio seguro de dados ao servidor** e o **armazenamento correto das assinaturas**. Abaixo na Figura 6, há um fluxograma do comportamento do Gerenciamento de Assinaturas que foi utilizado como modelo Esperado de sua funcionalidade *front-end*.

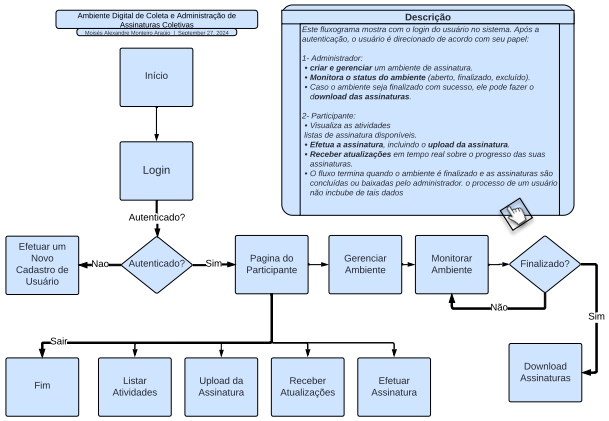


Figura 6 – Fluxograma do Gerenciamento de Assinaturas. Fonte: (MONTEIRO, Moisés, 2024d)

5.1.2 Usabilidade Esperada

A interface do sistema, desenvolvida com *Expo*(EXPO COMMUNITY, 2024), deve apresentar boa responsividade e facilidade de uso para os usuários. A navegação deve ser intuitiva, e as funcionalidades principais, como cadastro, login, captura de assinatura e visualização de dados, devem ser facilmente acessíveis e utilizáveis pelos usuários.

5.1.3 Usabilidade Esperada

A interface do sistema, desenvolvida com *Expo* (EXPO COMMUNITY, 2024), deve apresentar boa responsividade e facilidade de uso para os usuários. A navegação deve ser intuitiva, e as funcionalidades principais, como cadastro, login, captura de assinatura e visualização de dados, devem ser facilmente acessíveis e utilizáveis pelos usuários.

5.1.3.1 *Login*

O processo de *login* está simples e direto, permitindo que os usuários acessem a plataforma rapidamente com uma interface para maior conveniência e segurança,

singularmente usufruindo do o serviço *Clerk* (**ClerkOAuth2024**), conforme é ilustrado na Figura 7 abaixo.

Figura 7 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a)

5.1.3.2 Captura de Assinatura

Os usuários poderão visualizar sua assinatura no perfil do usuário, podendo alterar o próprio dado, porém caso haja alguma interação com algum ambiente de assinaturas, será validado assinatura do momento ocorrido, caso altere, o dado coletado sobre sua assinatura não será alterado, a menos que o mesmo faça posteriormente caso haja necessidade, a metodologia segue o padrão conforme na figura 8 abaixo para o envio de sua assinatura.

Figura 8 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a)

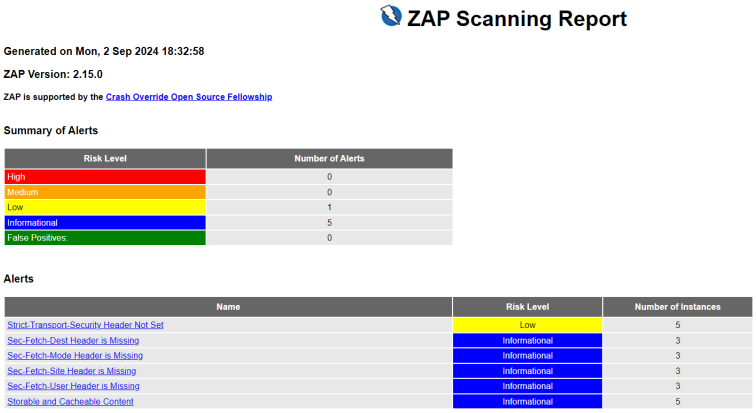
5.1.3.3 Visualização de Dados

Os usuários administrador poderão visualizar o gerenciamento dos dados coletados e os mesmo estarão cláros e organizados. A navegação de ambas as etapas poderão ser filtradas, conforme a necessidade da busca, garantindo que os usuários encontrem as informações desejadas de forma rápida e eficiente. Quando finalizado o gerenciamento, terá um modal de confirmação, após a confirmação, o ambiente estará preparado para coleta e download dos mesmos dados,no momento apenas a nível de *web*, assim ilustrado como na Figura 9 abaixo.

Figura 9 – Login Fonte: (MONTEIRO, Moises, 2024b) (MONTEIRO, Moises, 2024a)

5.1.4 Segurança Esperada

A segurança do sistema será avaliada utilizando a ferramenta OWASP ZAP (Zed Attack Proxy) para identificar e mitigar possíveis vulnerabilidades. Espera-se que o sistema seja capaz de proteger contra ataques cibernéticos, como Cross-Site Scripting (XSS) e Clickjacking, por meio da implementação de cabeçalhos de segurança HTTP, como Content Security Policy (CSP), Strict-Transport-Security (HSTS), e X-Frame-Options, novos testes foram feitos, com atualização dos resultados ilustrados abaixo na Figura 10, levando para zero *Number of Alerts* no *Risk Levels Medium*.



ZAP Scanning Report

Generated on Mon, 2 Sep 2024 18:32:58

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	1
Informational	5
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Strict-Transport-Security Header Not Set	Low	5
Sec-Fetch-Dest Header is Missing	Informational	3
Sec-Fetch-Mode Header is Missing	Informational	3
Sec-Fetch-Site Header is Missing	Informational	3
Sec-Fetch-User Header is Missing	Informational	3
Storable and Cacheable Content	Informational	5

Figura 10 – ZAP Scanning Report - expected results

Fonte: (FOUNDATION, O., 2024)(LLC, N., 2024)

Essas melhorias esperadas visam aumentar a resiliência do sistema contra ameaças cibernéticas, reforçando a sua proteção contra possíveis vetores de ataque e assegurando um ambiente seguro para o gerenciamento de assinaturas digitais.

Com base nas necessidades identificadas durante o desenvolvimento do sistema e nos objetivos do projeto, foram levantadas algumas expectativas em relação aos principais benefícios que o sistema poderá oferecer. As vantagens listadas a seguir são resultado de uma análise das funcionalidades implementadas e dos desafios enfrentados ao longo do processo de desenvolvimento. Espera-se que o sistema apresente as seguintes vantagens:

- **Eficiência na Gestão de Assinaturas**:O sistema facilitará o gerenciamento de assinaturas digitais, eliminando a necessidade de processos manuais e diminuindo o tempo requerido para as tarefas de coleta e armazenamento de assinaturas.
- **egurança e Privacidade**: A implementação de controle de acesso baseado em autenticação por *tokens*, juntamente com a opção de adicionar senhas a documentos sensíveis, deve assegurar a proteção das informações.
- **Flexibilidade e Controle**: O sistema permitirá que os administradores gerenciem e controlem o acesso às assinaturas, além de ajustar o nível de segurança conforme necessário.
- **Facilidade de Uso e Acessibilidade**: A interface, desenvolvida com *Expo*(EXPO COMMUNITY, 2024), foi projetada para ser amigável e responsiva, facilitando seu uso na *web* e permitindo futuras expansões para dispositivos móveis.

5.2 LIMITAÇÕES ESPERADAS

Apesar das vantagens mencionadas, durante o desenvolvimento foram identificadas algumas limitações no sistema que podem impactar sua funcionalidade ou a experiência do usuário. As principais limitações previstas são:

- **Funcionalidade Limitada ao Ambiente Web:** No estágio atual, o sistema foi desenvolvido com foco no ambiente *web*. Embora haja a possibilidade de expansão para dispositivos móveis, a utilização em plataformas como *Android e iOS* ainda não foi implementada, o que limita a acessibilidade para usuários que preferem essas plataformas.
- **Dependência de Conectividade Constante:** O sistema depende de uma conexão estável com a internet para operar corretamente. Em ambientes com baixa conectividade ou com falhas constantes, a experiência do usuário pode ser comprometida, especialmente em processos de assinatura ou sincronização de dados.
- **Falta de Equipamentos para Desenvolvimento e Teste em iOS:** A ausência de dispositivos *Apple* limitou o desenvolvimento e teste em tempo real para *iOS*, restringindo o alcance do projeto.

5.3 POSSIBILIDADES DE MELHORIAS FUTURAS

Baseadas nas expectativas iniciais, algumas melhorias futuras foram identificadas:

- **Expansão para Dispositivos Móveis**: Desenvolver versões compatíveis com Android e iOS utilizando Expo(EXPO COMMUNITY, 2024) para oferecer uma experiência multiplataforma completa.
- **Otimização do Armazenamento de Imagens**: Considerar alternativas para o armazenamento de imagens de assinaturas que possam ser mais eficientes em termos de espaço e processamento.
- **Implementação de Novas Funcionalidades**: Adicionar funcionalidades como notificações, relatórios detalhados de atividades e maior personalização de acesso para usuários e administradores.

5.4 CONSIDERAÇÕES FINAIS SOBRE OS RESULTADOS ESPERADOS

Os resultados esperados indicam que o sistema poderá proporcionar um ambiente seguro, eficiente e flexível para o gerenciamento de assinaturas digitais em

ambientes acadêmicos e administrativos. Embora algumas limitações tenham sido identificadas, há um bom potencial de crescimento e melhorias para o futuro.

6 DISCUSSÃO

Este capítulo discute os resultados alcançados com o desenvolvimento do sistema de gerenciamento de assinaturas digitais, abordando suas vantagens, os desafios enfrentados e seu posicionamento em relação a outras soluções disponíveis no mercado. Também são apresentadas reflexões sobre a eficácia do sistema, suas limitações e possíveis melhorias para futuras versões.

6.1 COMPARAÇÃO COM SOLUÇÕES EXISTENTES

O sistema desenvolvido se diferencia de outras soluções disponíveis no mercado ao oferecer flexibilidade em nível de desenvolvimento, permitindo integração com diversos processos sem comprometer a transparência das operações. Enquanto muitas plataformas prontas disponibilizam personalizações específicas para contextos institucionais particulares, o sistema proposto adota uma abordagem uniforme que assegura clareza e segurança na troca de informações entre usuários.

O uso de tecnologias modernas, como o Expo para o front-end e o Django REST Framework(DJANGO SOFTWARE FOUNDATION, 2024) (DRF) para o back-end, proporciona uma integração fluida e um suporte robusto ao desenvolvimento contínuo. A utilização da API externa Clerk(INC., C., 2024) para autenticação também fortalece a segurança, facilitando logins seguros por meio de métodos de autenticação amplamente utilizados, como o Google(LLC, G., 2024), sem se concentrar em particularidades de cada organização.

Essa combinação de tecnologias cria uma estrutura sólida de transparência e segurança na gestão de assinaturas digitais, assegurada pela simplicidade e robustez a nível de código. O *Django*, reconhecido por suas boas práticas de segurança, facilita a implementação de padrões criptográficos avançados, como o uso do algoritmo de *hash SHA-256*. Esse algoritmo é essencial para garantir a integridade dos dados, especialmente no armazenamento de senhas e dados sensíveis. O *SHA-256*, parte da família *Secure Hash Algorithm (SHA-2)*, gera uma sequência de 256 bits de dados, tornando-o altamente seguro e resistente a ataques de colisão, prevenindo que dois conjuntos de dados diferentes produzam o mesmo *hash* (STANDARDS; TECHNOLOGY, 2015).

Além disso, o *Django Rest Framework (DRF)*, combinado com autenticação por tokens e o protocolo *OAuth 2.0*, permite que a plataforma mantenha um nível elevado de controle de acesso e proteção dos dados (DJANGO SOFTWARE FOUNDATION, 2024). O sistema, projetado com uma abordagem de segurança em camadas, também

se beneficia da criptografia *AES (Advanced Encryption Standard)* para proteger os dados em trânsito e em repouso (DAEMEN; RIJMEN, 2001). Isso assegura que apenas usuários autorizados possam acessar as informações, promovendo um ambiente de confiança. A combinação dessas ferramentas e práticas não só torna a segurança robusta, mas também fácil de manter a nível de código, permitindo que administradores se concentrem nas funcionalidades sem comprometer a segurança (CLERK, 2024).

6.2 IMPLICAÇÕES PRÁTICAS

A implementação deste sistema traz implicações práticas relevantes para ambientes acadêmicos e administrativos. A digitalização das assinaturas torna o gerenciamento de documentos mais eficiente, reduzindo o tempo e o esforço necessários para coletar e organizar assinaturas. Esse processo automatizado permite que as instituições redirecionem recursos para atividades mais estratégicas, minimizando a burocracia e facilitando o gerenciamento de documentos.

A possibilidade de visualizar as informações dos responsáveis pela coleta de assinaturas, como nome, e-mail e foto, promove uma relação de confiança entre os participantes, fator crucial nesses ambientes. A capacidade de restringir o acesso a documentos específicos através de senhas fortalece a privacidade e a segurança das informações sensíveis, prevenindo acessos não autorizados e permitindo um maior controle sobre o processo de assinatura.

Embora o sistema não aborde particularidades específicas de cada instituição, ele é eficaz em múltiplos contextos, desde universidades até órgãos administrativos que gerenciam documentos que requerem múltiplas assinaturas.

6.3 LIMITAÇÕES DO SISTEMA

Apesar das vantagens apresentadas, o sistema possui algumas limitações. No momento, sua funcionalidade está restrita ao ambiente web, o que limita seu uso em dispositivos móveis. No entanto, a escolha pelo Expo como framework de desenvolvimento abre a possibilidade de expansão futura para plataformas móveis, como Android, ampliando o alcance e proporcionando uma experiência de usuário mais abrangente.

Outra limitação está no uso de imagens para entrega ao usuário final. Quando é feita uma requisição via API para download, onde ficam armazenadas as assinaturas referentes ao usuário administrador, embora essa abordagem seja funcional no escopo atual, ela está limitada a ser usufruída apenas pelo lado do cliente. Versões futuras do sistema poderiam adotar métodos que permitam a edição de documentos de forma eficiente ou utilizar serviços especializados de armazenamento em nuvem para esses dados.

A dependência da API externa Clerk(INC., C., 2024) para autenticação, apesar de oferecer recursos avançados de segurança, é um ponto que requer atenção. A utilização de um serviço externo demanda monitoramento contínuo quanto à sua disponibilidade e custo a longo prazo, além de potenciais alterações nas políticas do provedor.

6.4 POSSIBILIDADES DE MELHORIAS FUTURAS

Considerando as limitações identificadas e as oportunidades de desenvolvimento, algumas melhorias para futuras versões do sistema incluem:

- **Expansão para Plataformas Móveis:** Utilizar o Expo para desenvolver versões do sistema compatíveis com Android, aumentando o alcance e a acessibilidade para diversos dispositivos e contextos de uso.
- **Otimização de Armazenamento:** Migrar para métodos mais eficientes de armazenamento de assinaturas, como o uso de formatos de imagem compactos ou serviços de armazenamento em nuvem, aprimorando o desempenho e a escalabilidade do sistema.
- **Novas Funcionalidades de Segurança:** Implementar recursos como autenticação multifator (MFA) para reforçar a proteção contra acessos não autorizados e mecanismos de auditoria para registrar todas as atividades relacionadas às assinaturas digitais.
- **Melhoria na Experiência do Usuário:** Integrar notificações em tempo real, relatórios de uso detalhados e outras ferramentas de gestão que melhorem a usabilidade e ofereçam maior controle ao usuário final.
- **Monetização e Controle Financeiro:** Desenvolver funcionalidades para monetização do sistema, como planos de assinatura com diferentes níveis de acesso, garantindo a sustentabilidade a longo prazo.

6.5 CONSIDERAÇÕES FINAIS

O sistema de gerenciamento de assinaturas digitais demonstrou ser uma solução robusta e segura para os desafios enfrentados em ambientes acadêmicos e administrativos. Apesar de algumas limitações que precisam ser abordadas, as sugestões para futuras melhorias indicam um grande potencial para crescimento e evolução do sistema. As expansões planejadas reforçam o compromisso com uma solução de alta qualidade, que permanece confiável e transparente para todos os usuários, mesmo sem atender a particularidades institucionais específicas.

7 CONCLUSÃO

Este trabalho desenvolveu um sistema de gerenciamento de assinaturas digitais para ambientes acadêmicos e administrativos, oferecendo uma solução mais eficiente, segura e transparente para coleta e armazenamento de assinaturas.

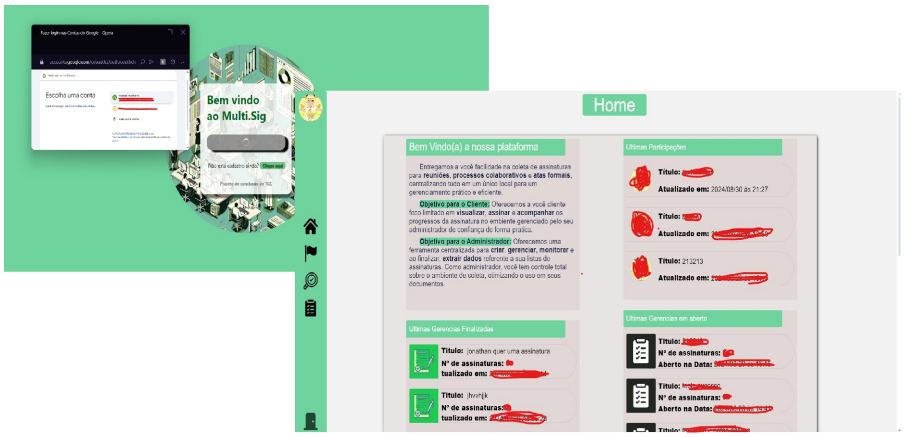


Figura 11 – Conclusão Projeto

7.1 RESUMO DOS PRINCIPAIS RESULTADOS

O sistema desenvolvido alcançou os objetivos propostos, fornecendo uma plataforma que facilita a coleta, o armazenamento e o gerenciamento de assinaturas digitais. A interface, construída com o Expo(INC., C., 2024), mostrou-se eficaz no ambiente web, proporcionando aos usuários uma experiência intuitiva e fluida. O uso do Django REST Framework (DRF)(DJANGO SOFTWARE FOUNDATION, 2024) no back-end assegurou uma comunicação eficiente e segura entre o cliente e o servidor, garantindo a robustez necessária para as operações de autenticação e gestão de assinaturas.

Adicionalmente, o sistema inclui funcionalidades importantes, como o controle de acesso e o consumo dos end-points por meio do uso do token do usuário, reforçando a privacidade, a segurança e a transparência no compartilhamento de informações entre os usuários, promovendo confiança mútua entre os participantes.

7.2 CONTRIBUIÇÕES DO TRABALHO

As principais contribuições deste trabalho incluem a criação de um sistema simplificado para o gerenciamento de assinaturas digitais. Ele oferece uma estrutura sólida e uniforme que assegura a segurança e a transparência das operações. O desenvolvimento de uma plataforma expansível para diferentes dispositivos e a adoção

de práticas robustas de segurança reforçam a aplicabilidade do sistema em futuras otimizações, além da Web.

Este projeto também agrega valor à literatura existente ao demonstrar uma abordagem prática para o desenvolvimento de sistemas utilizando tecnologias modernas, como Expo e Django REST Framework (DRF). Como discutido por Elysa Freitas Ferreira(MELO, 2021), a pandemia acelerou a necessidade de soluções digitais robustas e seguras, destacando os desafios e oportunidades na implementação de assinaturas digitais. O trabalho enfatiza os benefícios e desafios de criar uma solução de assinatura digital independente, sem depender de infraestruturas externas.

7.3 LIMITAÇÕES E TRABALHOS FUTUROS

Apesar das conquistas alcançadas, o sistema apresenta algumas limitações. Atualmente, sua funcionalidade é restrita ao ambiente web, o que limita seu alcance e usabilidade para usuários de dispositivos móveis.

Para trabalhos futuros, considera-se a expansão do sistema para plataformas móveis, como Android, utilizando as capacidades do Expo(INC., C., 2024) para oferecer uma experiência verdadeiramente multiplataforma. Outras melhorias propostas incluem a implementação de funcionalidades avançadas, como autenticação multifator, notificações personalizadas e auditoria de atividades, que poderiam aumentar ainda mais a usabilidade e a segurança do sistema.

7.4 CONSIDERAÇÕES FINAIS

Este trabalho apresentou o desenvolvimento de um sistema de gerenciamento de assinaturas digitais. Para aqueles que desejam explorar o código-fonte e entender mais detalhadamente a implementação, os repositórios do projeto estão disponíveis publicamente em:

- **Repositório Front-End:** `https://github.com/MoisesMonter/signature_front`
- **Repositório Back-End:** `https://github.com/MoisesMonter/signature_back`

A disponibilização do código permite maior transparência e contribui para futuras melhorias e expansões.

O desenvolvimento de um sistema próprio para o gerenciamento de assinaturas digitais revelou-se uma solução eficaz para os desafios enfrentados em ambientes acadêmicos e administrativos. As funcionalidades implementadas, aliadas à flexibilidade e adaptabilidade do sistema, proporcionam maior controle, segurança e eficiência no gerenciamento de assinaturas digitais.

Embora o sistema esteja em uma fase inicial, as propostas de melhorias futuras indicam um grande potencial para expansão e refinamento, tornando-o uma ferramenta ainda mais abrangente e útil para diversos contextos e usuários.

REFERÊNCIAS

(IETF), Internet Engineering Task Force. **HTTP Strict Transport Security (HSTS)**. [S.l.: s.n.], 2012. RFC sobre o HSTS, descrevendo seu funcionamento para garantir a segurança de conexões HTTPS. Disponível em: https://tools.ietf.org/html/rfc6797.

_____. **Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content**. [S.l.: s.n.], 2014. RFC sobre o protocolo HTTP, detalhando sua estrutura e funcionamento. Disponível em: https://tools.ietf.org/html/rfc7231.

_____. **The X-Frame-Options HTTP Response Header**. [S.l.: s.n.], 2010. RFC detalhando o uso do cabeçalho X-Frame-Options para proteger contra ataques de Clickjacking. Disponível em: https://tools.ietf.org/html/rfc7034.

ACRONIS. **Enhancing Business Efficiency with eSignatures: Key Advantages and Implementation Tips**. [S.l.: s.n.], 2024. Acesso em: 25 set. 2024. Disponível em: https://www.acronis.com/en-us/blog/posts/esignatures-key-advantages-and-implementation-tips/.

AL., Timo Furrer et. **drf-spectacular: Sane and flexible OpenAPI 3.0 schema generation for Django REST framework**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://drf-spectacular.readthedocs.io/. Acesso em: 31 ago. 2024.

BRASIL. **Lei nº 14.063, de 23 de setembro de 2020**. [S.l.: s.n.]. Acesso em: 25 set. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14063.htm.

BRASIL, Colégio Notarial do. A prática dos Cartórios de Notas no meio eletrônico: um avanço e modernização pelo e-notariado. **Blog Notarial**, 2020. Acesso em: 25 set. 2024. Disponível em: https://www.notariado.org.br.

CERTINAL. **The Evolution of E-Signatures: From Wet Ink to Digital Innovation**. [S.l.: s.n.], 2024. Acesso em: 25 set. 2024. Disponível em: https://www.certinal.com/blog/the-evolution-of-esignatures-from-wet-ink-to-digital-innovation.

CLERK. **Security Overview: Clerk API**. [S.l.: s.n.], 2024. https://clerk.dev/docs/security. Acesso em: 25 set. 2024.

DAEMEN, Joan; RIJMEN, Vincent. **AES Algorithm: Advanced Encryption Standard**. [S.l.: s.n.], 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Acesso em: 25 set. 2024.

DJANGO SOFTWARE FOUNDATION. **Django REST Framework**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://www.django-rest-framework.org/. Acesso em: 31 ago. 2024.

DONIZETTI, Elpídio. A segurança jurídica das assinaturas digitais e a criptografia assimétrica. **Jus Navigandi**, 2020. Acesso em: 25 set. 2024. Disponível em: https://jus.com.br/artigos/.

DRYSIGN. **E-signatures: Optimizing document workflow automation**. [S.l.: s.n.], 2024. Acesso em: 25 set. 2024. Disponível em: https://www.drysign.exelatech.com/blog/optimizing-document-workflow-automation.

E-NOTARIADO. **e-notariado: plataforma oficial do notariado digital**. [S.l.: s.n.]. Acesso em: 25 set. 2024. Disponível em: https://www.e-notariado.org.br.

EXPO COMMUNITY. **Expo Documentation**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://docs.expo.dev/. Acesso em: 31 ago. 2024.

FOUNDATION, Django Software. **Django REST Framework - Authentication**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://www.django-rest-framework.org/api-guide/authentication/. Acesso em: 31 ago. 2024.

FOUNDATION, OWASP. **OWASP ZAP: Zed Attack Proxy**. [S.l.: s.n.], 2024. Ferramenta de código aberto para testes de segurança dinâmica de aplicações web, utilizada para detectar vulnerabilidades como injeção de SQL, cross-site scripting (XSS) e exposição de informações sensíveis. Disponível em: https://www.zaproxy.org.

GREATH APES, INC. **react-native-view-shot**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://www.npmjs.com/package/react-native-view-shot/v/1.9.1. Acesso em: 31 ago. 2024.

GUNAWAN, Indra et al. How the COVID-19 Pandemic Affected the Sustainable Adoption of Digital Signature: An Integrated Factors Analysis Model. **Sustainability**, v. 14, n. 7, p. 4281, 2022. Discussão sobre o impacto da pandemia na adoção de assinaturas digitais e seu crescimento sustentado. DOI: 10.3390/su14074281. Disponível em: https://doi.org/10.3390/su14074281.

HOSTING, Verpex. **Cross-Site Scripting (XSS) Prevention: A Detailed Web Security Checklist**. [S.l.: s.n.], 2024. Lista de práticas recomendadas para prevenção de ataques XSS e mitigação de vulnerabilidades em aplicações web. Disponível em: https://verpex.com/blog/privacy-security/cross-site-scripting-xss-prevention-a-detailed-web-security-checklist.

IGREE. **Reconhecer firma: veja como realizar o processo digitalmente**. [S.l.: s.n.], 2020. Acesso em: 25 set. 2024. Disponível em: https://www.igree.co.

INC., Clerk. **Clerk: A Modern Authentication and User Management Platform**. [S.l.: s.n.], 2024. Plataforma que oferece ferramentas para autenticação de usuários, login social, autenticação multifator, gerenciamento de sessão e recuperação de senha, otimizando a segurança digital para aplicativos web e mobile. Disponível em: https://clerk.dev.

INC., Splunk. **Cross-Site Scripting (XSS) & How to Prevent Attacks**. [S.l.: s.n.], 2024. Guia detalhado sobre a prevenção de ataques XSS e práticas recomendadas para segurança de aplicações web. Disponível em: https://www.splunk.com.

JOSEFSSON, Simon. **The Base16, Base32, and Base64 Data Encodings**. [S.l.: s.n.], 2006. https://www.rfc-editor.org/rfc/rfc4648. Acesso em: 25 set. 2024.

JUSTIÇA (CNJ), Conselho Nacional de. **Provimento nº 100 de 26 de maio de 2020**. [S.l.: s.n.], 2020. Acesso em: 25 set. 2024. Disponível em: https://atos.cnj.jus.br/files/original10468020200528392434provimento_100.pdf.

KRAWCZYK, Hugo; BELLARE, Mihir; CANETTI, Ran. HMAC: Keyed-Hashing for Message Authentication. **RFC 2104, Internet Engineering Task Force**, 1995. Acesso em: 25 set. 2024. Disponível em: https://www.rfc-editor.org/rfc/rfc2104.html.

LLC, Google. **Sign in with Google - Authentication for Web and Apps**. [S.l.: s.n.], 2024. Accessed: August 31, 2024. Disponível em: https://developers.google.com/identity/sign-in/web.

LLC, Identity. **What Are Digital Signatures? The Complete Guide**. [S.l.: s.n.], 2024. Guia completo sobre a importância das assinaturas digitais e suas aplicações em diversas áreas. Disponível em: https://www.identity.com/what-are-digital-signatures/.

LLC, Ngrok. **Ngrok: Secure Tunnels to Localhost**. [S.l.: s.n.], 2024. Serviço que permite a exposição segura de servidores locais na internet, útil para testes de desenvolvimento e integração contínua, como testes de segurança dinâmica e integração de APIs. Disponível em: https://ngrok.com.

MCGREW, David W. The use of Base64 for secure data storage and transmission. **Journal of Applied Cryptography**, 2018. Acesso em: 25 set. 2024. Disponível em: https://www.examplejournal.com.

MELO, Elysa Freitas Ferreira de. **Assinatura Digital e a Evolução da Tecnologia na Pandemia**. [S.l.: s.n.], 2021. Trabalho de Conclusão de Curso, Pontifícia Universidade Católica de Goiás.

META PLATFORMS, INC. **React Native**. Acesso em: 31 ago. 2024. 2024. Disponível em: https://reactnative.dev/. Acesso em: 31 ago. 2024.

MONTEIRO, Moisés. **Diagrama de Arquitetura C4-Context - Sistema de Gerenciamento de Assinaturas Digitais**. [S.l.: s.n.], 2024. https://l1nq.com/5bLmX. Acesso em: 25 set. 2024.

_____. **Diagrama de Caso de Uso - Sistema de Gerenciamento de Assinaturas Digitais**. [S.l.: s.n.], 2024. https://l1nq.com/oXbtT. Acesso em: 25 set. 2024.

_____. **Diagrama do Banco de Dados - Sistema de Gerenciamento de Assinaturas Digitais**. [S.l.: s.n.], 2024. https://l1nq.com/g0mm3. Acesso em: 25 set. 2024.

_____. **Gerência de Assinaturas - Fluxograma**. [S.l.: s.n.], 2024. Fluxograma explicativo sobre o gerenciamento de assinaturas digitais, utilizado em TCC. Disponível em: https://encurtador.com.br/8R7Cy.

MONTEIRO, Moises. **signature_back: Backend para Sistema de Gerenciamento de Assinaturas Digitais**. [S.l.: s.n.], 2024. https://github.com/MoisesMonter/signature_back. Repositório GitHub para o backend do sistema de gerenciamento de assinaturas digitais desenvolvido em Django Rest Framework (DRF).

_____. **signature_front: Frontend para Sistema de Gerenciamento de Assinaturas Digitais**. [S.l.: s.n.], 2024. https://github.com/MoisesMonter/signature_front.git. Repositório GitHub para o front-end do sistema de gerenciamento de assinaturas digitais, desenvolvido com React Native e Expo.

NAVIGANDI, Jus. CNJ e o tabelião digital: evolução dos cartórios em tempos de pandemia. **Jus.com.br**, 2020. Acesso em: 25 set. 2024. Disponível em: https://jus.com.br/artigos/.

PROVOS, Niels; MAZIÈRES, David. A Future-Adaptable Password Scheme. **USENIX Annual Technical Conference**, 1999. Acesso em: 25 set. 2024. Disponível em: https://www.usenix.org/legacy/event/usenix99/provos.html.

RIVEST, R. **The MD5 Message-Digest Algorithm (RFC 1321)**. [S.l.], 1992. Disponível em: https://tools.ietf.org/html/rfc1321.

SANTOS MACHADO, Cristiano dos. A evolução das assinaturas digitais no Brasil. **Revista de Direito Digital**, v. 5, n. 1, p. 34–45, 2020.

SCHNEIER, Bruce. **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. 2nd. New York: Wiley Publishing, 1996.

SILVA, Fernando Lopes. A transformação digital no Brasil impulsionada pela pandemia: o papel das assinaturas digitais. **Revista de Direito e Tecnologia**, v. 12, n. 2, p. 22–30, 2021.

STANDARDS, National Institute of; TECHNOLOGY. **SHA: Secure Hash Standard (FIPS PUB 180-4)**. [S.l.], 2015. Disponível em: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

W3C. **Content Security Policy (CSP) Level 3**. [S.l.: s.n.], 2021. Guia oficial sobre a implementação da política de segurança CSP. Disponível em: https://www.w3.org/TR/CSP3/.