Universidade de Brasília - UnB

Faculdade de Ciências e Tecnologias em Engenharia – FCTE

Engenharia de Software

# AssinApp: Aplicativo mobile para assinatura digital de documentos

Autor: Arthur Talles de Sousa Cunha, Eduardo Gurgel Pereira de Carvalho

Orientador: Prof. Dr. John L. Gardenghi

Brasília, DF

2025

Arthur Talles de Sousa Cunha, Eduardo Gurgel Pereira de Carvalho

# AssinApp: Aplicativo mobile para assinatura digital de documentos

Monografia submetida ao curso de graduação em Engenharia de Software da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Software .

Universidade de Brasília - UnB

Faculdade de Ciências e Tecnologias em Engenharia – FCTE

Orientador: Prof. Dr. John L. Gardenghi

Brasília, DF

2025

Arthur Talles de Sousa Cunha, Eduardo Gurgel Pereira de Carvalho
AssinApp: Aplicativo mobile para assinatura digital de documentos/ Arthur Talles de Sousa Cunha, Eduardo Gurgel Pereira de Carvalho. – Brasília, DF, 2025- ’ 109 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. John L. Gardenghi

Trabalho de Conclusão de Curso – Universidade de Brasília - UnB
Faculdade de Ciências e Tecnologias em Engenharia – FCTE , 2025.

1. Desenvolvimento, App. 2. Assinatura digital. I. Prof. Dr. John L. Gardenghi. II. Universidade de Brasília. III. Faculdade UnB Gama. IV. AssinApp: Aplicativo mobile para assinatura digital de documentos

CDU 02:141:005.6

Arthur Talles de Sousa Cunha, Eduardo Gurgel Pereira de Carvalho

# AssinApp: Aplicativo mobile para assinatura digital de documentos

Monografia submetida ao curso de graduação em Engenharia de Software da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Engenharia de Software .

Trabalho aprovado. Brasília, DF, 19 de fevereiro de 2025:

---

**Prof. Dr. John L. Gardenghi**
Orientador

---

**Prof. Dr. Bruno César Ribas**
Convidado 1

---

**Prof. Dr. Glauco Vitor Pedrosa**
Convidado 2

Brasília, DF
2025

# Agradecimentos

A realização deste trabalho foi possível graças ao apoio e incentivo de diversas pessoas, às quais expressamos nossa profunda gratidão.

Em primeiro lugar, agradecemos a Deus, por nos conceder força e perseverança durante toda essa jornada.

Além disso, somos imensamente gratos a nossos familiares, pelo suporte incondicional, paciência e palavras de encorajamento nos momentos mais desafiadores.

Também estendemos nossa gratidão a nosso orientador, Prof. Dr. John Lenon Gardenghi, por sua dedicação, ensinamentos e valiosas contribuições, que foram fundamentais para a construção deste trabalho.

Da mesma forma, agradecemos aos colegas e amigos, pelo compartilhamento de conhecimentos, apoio mútuo e incentivo constante ao longo do desenvolvimento deste projeto.

Adicionalmente, reconhecemos o papel de todos os professores do curso, cujos ensinamentos foram essenciais para nossa formação acadêmica e profissional.

Por fim, a todos que, de alguma forma, contribuíram para a concretização deste trabalho, nosso sincero muito obrigado.

*"Se vi mais longe, foi por estar sobre os ombros de gigantes."*
*(— Isaac Newton)*

# Resumo

O presente trabalho de conclusão de curso (TCC) apresenta o desenvolvimento de um aplicativo de assinatura digital, focado em oferecer uma solução mobile para a assinatura, buscando a validação e autenticação de documentos digitais. Com a crescente demanda da digitalização de processos e a necessidade de reduzir o uso de papel, a implementação de assinaturas digitais tornou-se essencial em diversas áreas, como em Universidades, administração pública e também na área jurídica. O desenvolvimento do aplicativo foi conduzido utilizando metodologias ágeis, com ênfase em entregas incrementais. A plataforma escolhida para o desenvolvimento foi o React Native, aproveitando sua eficiência e flexibilidade para a criação de aplicativos no ambiente Android, garantindo maior produtividade e economia de recursos.

**Palavras-chaves**: Assinatura Digital, Segurança, Criptografia, Aplicativo Móvel, React Native, Autenticação.

# Abstract

This final course project (TCC) presents the development of a digital signature application, focused on providing a mobile solution for signing, validating, and authenticating digital documents. With the growing demand for process digitalization and the need to reduce paper usage, the implementation of digital signatures has become essential in various fields, such as universities, public administration, and the legal sector. The development of the application was conducted using agile methodologies, with an emphasis on incremental deliveries. The platform chosen for development was React Native, leveraging its efficiency and flexibility for building applications in the Android environment, ensuring greater productivity and resource savings.

**Key-words**: Digital Signature, Security, Cryptography, Mobile Application, React Native, Authentication.

# Lista de ilustrações

# Lista de tabelas

# Lista de abreviaturas e siglas

| | |
|---|---|
| API | Application Programming Interface |
| CA | Autoridade Certificadora |
| CI/CD | Continuous Integration / Continuous Deployment |
| DER | Diagrama de Entidade e Relacionamento |
| ETSI | European Telecommunications Standards Institute |
| ESB | Enterprise Service Bus |
| ICP | Infraestrutura de Chaves Públicas |
| JAWS | Job Access With Speech |
| MFA | Multi-Factor Authentication |
| NVDA | NonVisual Desktop Access |
| PKI | Public Key Infrastructure |
| REST | Representational State Transfer |
| TCSEC | Trusted Computer System Evaluation Criteria |
| UX | User Experience |
| WAI | Web Accessibility Initiative |
| WCAG | Web Content Accessibility Guidelines |
| JWT | JSON Web Token |
| PDF | Portable Document Format |
| AWS | Amazon Web Services |
| STJ | Superior Tribunal de Justiça |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| OpenSSL | Open Source Secure Sockets Layer |
| TLS | Transport Layer Security |

| | |
|---|---|
| SSL | Secure Sockets Layer |
| IDAS | Identificação e Autenticação de Sistema |
| eIDAS | Electronic Identification, Authentication and Trust Services |
| RF | Requisitos Funcionais |
| RNF | Requisitos Não Funcionais |
| EAP | Estrutura Analítica do Projeto |
| URL | Uniform Resource Locator |
| UI | User Interface |
| UX/UI | User Experience / User Interface |
| MER | Modelo Entidade-Relacionamento |
| SGBD | Sistema de Gerenciamento de Banco de Dados |
| US$ | Dólar Americano |
| R$ | Real (currency) |
| IP | Infraestrutura de Provedor |
| TCC1 | Trabalho de Conclusão de Curso 1 |
| TCC2 | Trabalho de Conclusão de Curso 2 |
| XP | Extreme Programming |

# Sumário

# 1 Introdução

No cenário atual, a segurança e a autenticidade das transações eletrônicas são de extrema importância. Com o crescimento exponencial do uso de dispositivos móveis e a digitalização de processos, a necessidade de garantir que as informações transmitidas eletronicamente sejam autênticas e íntegras se torna cada vez mais crucial. As assinaturas digitais surgem como uma solução robusta para essa necessidade, proporcionando uma forma segura de verificar a identidade do remetente e a integridade da mensagem.

Este trabalho teve como objetivo implementar uma solução mobile para realizar assinatura digital em documentos, destacando os principais conceitos, tecnologias e ferramentas que suportaram esse processo.

## 1.1 Contextualização

A assinatura digital é uma técnica criptográfica que permite verificar a autenticidade e a integridade de documentos digitais. De acordo com Instituto Nacional de Padrões e Tecnologia (2013), a assinatura digital é gerada utilizando uma chave privada que corresponde a uma chave pública disponível para qualquer interessado em verificar a assinatura. Esta tecnologia tem se mostrado essencial em diversos setores, incluindo o governo, as finanças e o comércio eletrônico, onde a segurança da informação é primordial (TOLMASQUIM, 2012).

Conforme define European Telecommunications Standards Institute (2015), a assinatura digital trata de um conjunto de dados eletrônicos que acompanham ou estão logicamente associados a outros dados eletrônicos, utilizados como método de autenticação da informação. Isso garante que os dados não foram alterados desde que foram assinados e que a assinatura só pode ser gerada pelo signatário.

Com a crescente adoção de dispositivos móveis, a implementação de assinaturas digitais em aplicativos mobile apresenta desafios específicos. Esses desafios incluem a gestão segura de chaves em dispositivos que podem ser facilmente perdidos ou comprometidos, e a necessidade de interfaces de usuário intuitivas que facilitem a assinatura de documentos digitais (ZHANG; LI, 2010).

Além disso, a importância de uma infraestrutura de chave pública (PKI) bem estabelecida é fundamental para a verificação das assinaturas digitais. A PKI fornece os mecanismos necessários para a emissão, gerenciamento e revogação de certificados digitais, que são essenciais para garantir a confiança nas assinaturas digitais (HOUSLEY; POLK, 2001a).

Neste contexto, este trabalho visou explorar as ferramentas e técnicas necessárias para a implementação eficiente de assinaturas digitais em aplicativos mobile. A seguir, serão discutidos os fundamentos teóricos das assinaturas digitais, as ferramentas tecnológicas que suportam esse processo e as melhores práticas para garantir a segurança e a usabilidade das soluções desenvolvidas.

## 1.2 Objetivos

No presente trabalho, a construção de uma solução de assinatura digital em um aplicativo móvel demandou uma abordagem estruturada, onde os objetivos foram estabelecidos em diferentes níveis. Primeiramente, definiu-se o objetivo geral, que descreve a finalidade ampla do projeto, estabelecendo a direção e os resultados esperados de forma abrangente. Em seguida, delinearam-se os objetivos específicos, que detalham as etapas concretas e os requisitos técnicos necessários para alcançar o objetivo maior, assegurando que todas as partes do projeto estivessem alinhadas e contribuíssem para o desenvolvimento do aplicativo.

### 1.2.1 Objetivo geral

O objetivo deste trabalho foi desenvolver uma solução de assinatura digital em um aplicativo móvel. A solução buscou ser segura, eficiente e fácil de usar, proporcionando uma experiência de usuário intuitiva e confiável.

Para alcançar este objetivo, foram exploradas e aplicadas diversas tecnologias e ferramentas, incluindo criptografia assimétrica[1], certificados digitais[2] e infraestruturas de chave pública (PKI)[3].

### 1.2.2 Objetivo específico

Para atingir o objetivo geral deste trabalho, foram definidos os seguintes objetivos específicos:

- Utilizar uma arquitetura de certificados digitais e PKI: Adotar uma arquitetura existente de certificados digitais e infraestruturas de chave pública (PKI) para garantir a segurança do aplicativo.
- Implementar o protótipo do aplicativo móvel: Desenvolver e testar um protótipo funcional do aplicativo móvel, integrando a solução de assinatura digital e garantindo que ele seja intuitivo e fácil de usar.

[1] https://cloud.google.com/kms/docs/asymmetric-encryption?hl=pt-br. Acessado em 24/01/2025.
[2] https://www.gov.br/pt-br/servicos/obter-certificacao-digital. Acessado em 24/01/2025.
[3] https://www.entrust.com/pt/resources/learn/what-is-pki. Acessado em 24/01/2025.

- Documentar e avaliar a solução: Elaborar uma documentação detalhada do processo de desenvolvimento, das tecnologias utilizadas e dos resultados obtidos.

## 1.3 Organização do Trabalho

Este trabalho está estruturado nos seguintes capítulos:

- **Capítulo 2 - Fundamentação Teórica:** apresenta os conceitos e teorias fundamentais ao tema, incluindo uma revisão da literatura e a explicação de conceitos-chave que sustentam o desenvolvimento do projeto.
- **Capítulo 3 - Suporte Tecnológico:** descreve as ferramentas e tecnologias utilizadas no desenvolvimento do aplicativo, abrangendo ferramentas de modelagem (Figma, Draw.io, LucidChart), desenvolvimento (React Native, Expo) e gerenciamento (Git).
- **Capítulo 4 - Metodologia:** especifica os aspectos metodológicos do trabalho, detalhando os métodos e técnicas utilizados, os procedimentos de coleta e análise de dados, e a justificativa das escolhas metodológicas.
- **Capítulo 5 - AssinApp:** apresenta em detalhes o aplicativo desenvolvido neste trabalho, abordando a criação de personas, análise de aplicativos similares, requisitos funcionais e não funcionais, estrutura analítica do projeto (EAP), arquitetura do sistema, identidade visual, diagramas de pacotes e plano de gerenciamento de custos.
- **Capítulo 6 - Conclusão:** sugere implementações e aprimoramentos futuros, além de considerações finais sobre o potencial de expansão do projeto.

# 2 Fundamentação Teórica

Neste capítulo, foram explorados os conceitos teóricos essenciais e as bases legais que sustentam o desenvolvimento de um aplicativo de assinatura digital. Foram abordados aspectos técnicos, como criptografia e segurança, bem como as implicações legais e regulatórias. Além disso, o capítulo também discutiu a usabilidade e as melhores práticas de implementação, oferecendo uma visão abrangente do contexto necessário para o desenvolvimento do aplicativo.

## 2.1 Documentos Digitais

Os documentos digitais são representações eletrônicas de informações que podem ser armazenadas, acessadas e transmitidas por meio de dispositivos digitais. Diferentemente dos documentos físicos, que dependem de materiais como papel e tinta, os documentos digitais existem em formatos eletrônicos que facilitam sua criação, modificação e distribuição, constituindo uma alternativa interessante e condizente com os processos de modernização e avanços tecnológicos pelos quais a humanidade atravessa (GANDINI; SALOMÃO; JACOB, 2001).

Apesar de vantagens, como a redução de custos com papel, maior eficiência no armazenamento e recuperação de informações, e a possibilidade de integração com outras tecnologias, o uso de documentos digitais também apresenta desafios. A segurança da informação é uma das principais preocupações, especialmente em relação à proteção contra acessos não autorizados e à garantia da autenticidade e integridade dos documentos Além disso, questões relacionadas à interoperabilidade e padronização de formatos digitais também são relevantes, dado o vasto número de softwares e plataformas disponíveis (SANTOS; FLORES, 2015).

No Brasil, a legalidade e validade dos documentos digitais são regidas por diversas normativas, como a Medida Provisória nº 2.200-2, que estabelece a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) (HAAS et al., 2022). Além disso, padrões internacionais, como o PDF/A, são amplamente adotados para assegurar a longevidade e preservação de documentos digitais (VITAL, 2011).

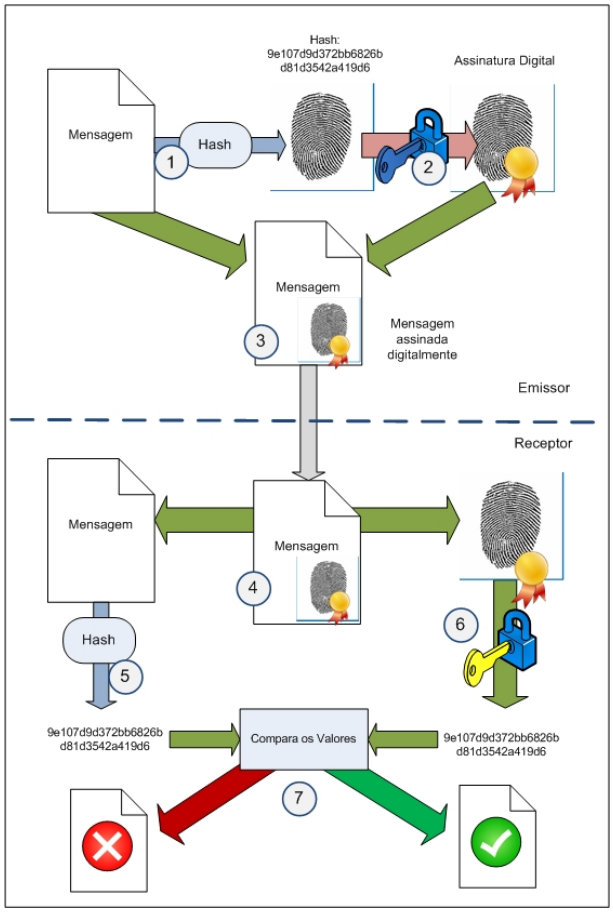
## 2.2 Assinatura Digital

Uma assinatura digital é uma técnica criptográfica que assegura a integridade e autenticidade de um documento digital. Segundo o National Institute of Standards and

Technology (NIST), uma assinatura digital é gerada utilizando uma chave privada, a qual está associada a uma chave pública correspondente. Qualquer parte interessada pode utilizar essa chave pública para verificar a autenticidade da assinatura digital (STANDARDS; (NIST), 2000).

A Figura 1 ilustra o processo de assinatura digital, demonstrando como a chave privada é utilizada para assinar o documento, enquanto a chave pública é empregada para verificar sua autenticidade.

Figura 1 – Assinatura Digital




*Fonte: Adaptado de Maciel (2008)*

De forma semelhante, a European Telecommunications Standards Institute (ETSI) define a assinatura digital como um conjunto de dados eletrônicos que acompanha ou está logicamente associado a outros dados eletrônicos, sendo empregado como método de autenticação da informação (LIPP, 2012).

### 2.2.1 Definição e Conceitos Básicos

Segundo Stallings (2017), a criptografia assimétrica, também conhecida como criptografia de chave pública, utiliza um par de chaves criptográficas: uma chave pública e uma chave privada. A chave pública é usada para criptografar e verificar assinaturas,

enquanto a chave privada é usada para descriptografar e criar assinaturas. Essa técnica é fundamental para a segurança das transações eletrônicas, especialmente em ambientes onde a confidencialidade e a autenticidade das informações são cruciais.

Kaufman, Perlman e Speciner (2016) explica que a criptografia assimétrica resolve o problema da distribuição de chaves na criptografia simétrica, permitindo que as chaves públicas sejam distribuídas abertamente, enquanto as chaves privadas permanecem secretas. Essa solução é essencial para o funcionamento seguro de sistemas de assinatura digital, como o proposto no aplicativo.

### 2.2.2 Certificados Digitais

Os certificados digitais são documentos eletrônicos emitidos por uma Autoridade Certificadora (CA) que vinculam uma chave pública a uma identidade específica. Eles desempenham um papel crucial na construção de uma Infraestrutura de Chaves Públicas (PKI), que é fundamental para garantir a segurança e autenticidade das comunicações eletrônicas. De acordo com Housley e Polk (2001b), esses certificados são essenciais para estabelecer uma PKI confiável, assegurando que as transações digitais ocorram de forma segura e autêntica.

Além disso, os certificados digitais permitem que as partes envolvidas em uma comunicação eletrônica verifiquem a autenticidade e a integridade das chaves públicas utilizadas. Adams e Lloyd (2003) destacam que, ao utilizar um certificado digital, uma entidade pode confiar que a chave pública associada ao certificado realmente pertence à pessoa ou organização identificada, tornando as transações eletrônicas mais seguras e protegidas contra fraudes.

No contexto de um aplicativo de assinatura digital, os certificados digitais garantem a autenticidade das assinaturas e a segurança das transações. Segundo Stallings (2006), a confiança em uma assinatura digital depende diretamente da credibilidade da Autoridade Certificadora que emitiu o certificado digital. Portanto, a escolha de uma CA respeitável e amplamente reconhecida é um fator importante para a segurança das aplicações de assinatura digital.

### 2.2.3 ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é um sistema de certificação digital estabelecido pelo governo brasileiro para garantir a autenticidade, integridade e validade jurídica de documentos eletrônicos. Criada pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, a ICP-Brasil é composta por uma hierarquia de autoridades certificadoras que emitem certificados digitais para pessoas físicas, jurídicas, aplicações e equipamentos, assegurando a identidade das partes envolvidas em transações

eletrônicas.

Embora os certificados emitidos sob a ICP-Brasil sejam amplamente utilizados em diversas aplicações governamentais e privadas, o Superior Tribunal de Justiça (STJ)[1], decidiu que a falta de credenciamento na ICP-Brasil não invalida automaticamente uma assinatura eletrônica. Dessa forma, sistemas privados também podem oferecer serviços de assinatura digital válidos, desde que garantam a autenticidade e a integridade dos documentos assinados.

## 2.3 Padrões e Protocolos de Segurança

A segurança em aplicativos de assinatura digital é garantida pelo uso de padrões e protocolos robustos, que protegem contra fraudes e ataques cibernéticos. A Public Key Infrastructure (PKI) é um sistema abrangente que oferece o suporte necessário para a segurança de aplicativos de assinatura digital. Segundo Stallings (2017), a PKI envolve um conjunto de funções, políticas e procedimentos para gerenciar o ciclo de vida dos certificados digitais, garantindo a confidencialidade, integridade e autenticidade das assinaturas digitais.

A utilização de certificados digitais facilita a implementação de autenticação multifator e assegura a validade jurídica das assinaturas eletrônicas, aumentando a segurança e a confiança dos usuários. A PKI é, portanto, essencial para a construção de um ambiente digital seguro e confiável.

## 2.4 Aspectos Legais

Os aspectos legais relacionados à utilização de aplicativos de assinatura digital são fundamentais para garantir a conformidade com a legislação vigente e proporcionar segurança jurídica aos usuários. A implementação de assinaturas digitais deve observar as leis e regulamentos que regem a validade jurídica dos documentos eletrônicos em diferentes jurisdições.

No Brasil, a Medida Provisória nº 2.200-2 de 2001[2] instituiu a ICP-Brasil, que regula o uso de assinaturas digitais e certifica a autenticidade, integridade e validade jurídica dos documentos eletrônicos. No entanto, conforme entendimento consolidado pelo STJ, assinaturas eletrônicas certificadas por entidades privadas também podem ser consideradas válidas, desde que atendam a requisitos de autenticidade e integridade.

[1] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/03122024-Falta-de-credenciamento-da-entidade-certificadora-na-ICP-Brasil--por-si-so--nao-invalida-assinatura-eletronica.aspx> . Acesso em: 30 jan. 2025.

[2] Disponível em: <https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 30 jan. 2025.

### 2.4.1 Validade Jurídica

A validade jurídica das assinaturas digitais é um dos principais aspectos a serem considerados ao utilizar um aplicativo de assinatura digital. Para que uma assinatura digital tenha validade jurídica, ela deve cumprir uma série de requisitos estabelecidos por leis e regulamentações específicas, como a utilização de certificados digitais emitidos por uma autoridade certificadora confiável.

Dessa forma, assinaturas eletrônicas podem ser aceitas em processos judiciais e administrativos, proporcionando segurança e confiança aos usuários, independentemente de serem certificadas pela ICP-Brasil ou por entidades privadas.

## 2.5 Segurança e Confiabilidade

### 2.5.1 Importância da Segurança em Aplicativos de Assinatura Digital

A segurança é um dos pilares fundamentais para qualquer sistema de assinatura digital, pois envolve a proteção de dados sensíveis e a garantia de que as assinaturas eletrônicas não possam ser falsificadas ou manipuladas. Em aplicativos móveis, onde as ameaças podem ser ainda mais variadas e complexas, garantir um alto nível de segurança é essencial para a confiabilidade do sistema e a confiança dos usuários (OTTONI, 2005).

### 2.5.2 Principais Ameaças e Riscos de Segurança

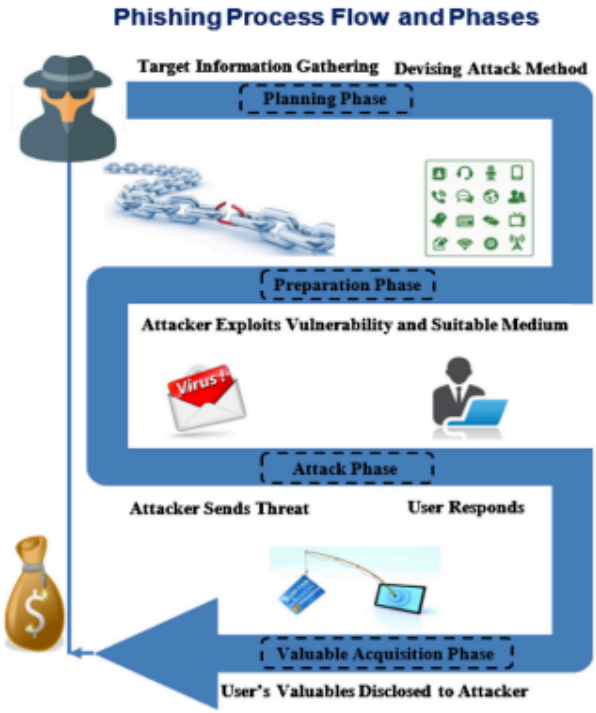
Os aplicativos móveis enfrentam diversos riscos de segurança que podem comprometer a integridade dos documentos assinados e a confiança dos usuários no sistema (BINE; KUK, 2016). A seguir, são descritas as principais ameaças e riscos associados:

#### 2.5.2.1 Ataques de Phishing

Os ataques de phishing envolvem a tentativa de enganar usuários para que revelem informações sensíveis, como credenciais de login, por meio de e-mails ou sites falsos que imitam a aparência de serviços legítimos (RAMZAN, 2010). Em aplicativos de assinatura digital, os atacantes podem enviar e-mails fraudulentos solicitando que o usuário forneça informações de acesso ou baixe malware que comprometa a segurança do dispositivo. Esses ataques podem resultar no roubo de informações pessoais e na manipulação não autorizada de documentos.

A Figura 2 ilustra o processo geral de um ataque de phishing, destacando as etapas envolvidas na tentativa de obter informações confidenciais de forma fraudulenta.

Figura 2 – Processo Geral de Ataque de Phishing



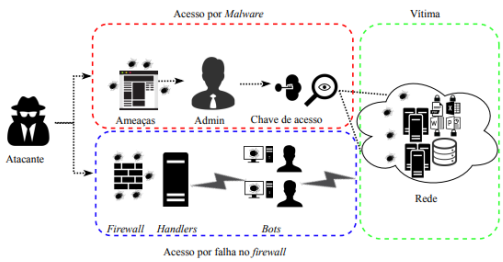

*Fonte: (ALKHALIL et al., 2021)*

#### 2.5.2.2 Malwares e Softwares Espiões

Malwares, incluindo vírus, worms e trojans, são programas maliciosos projetados para infiltrar e danificar sistemas. You e Yim (2010) afirma que em aplicativos móveis, o malware pode ser usado para capturar dados sensíveis, como chaves privadas usadas para assinar documentos, ou para comprometer a integridade dos arquivos de assinatura. Softwares espiões podem monitorar as atividades do usuário e coletar informações sem o seu consentimento, expondo-o a riscos adicionais.

A Figura 3 apresenta o funcionamento de um ataque por malware, mostrando como o software malicioso pode infectar dispositivos e comprometer dados críticos.

Figura 3 – Processo Geral de Ataque por Malware



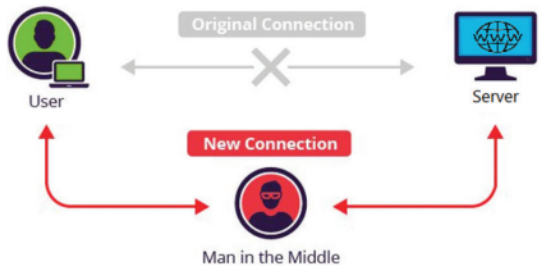

*Fonte: (MACIEL, 2018)*

#### 2.5.2.3 Ataques de Interceptação e Man-in-the-Middle

Ataques de man-in-the-middle (MitM) ocorrem quando um atacante intercepta a comunicação entre o usuário e o servidor para acessar, alterar ou redirecionar os dados (CONTI; DRAGONI; LESYK, 2016). Em aplicativos de segmentos semelhantes ao de assinatura digital, um ataque MitM pode permitir que o atacante visualize ou modifique o conteúdo dos documentos antes da assinatura, comprometendo a autenticidade da assinatura. A implementação de medidas de segurança, como a validação de certificados e a criptografia de ponta a ponta, é crucial para mitigar esses riscos (GREENWOOD; KHAN, 2014).

A Figura 4 demonstra uma arquitetura comum de ataque MitM, ilustrando como o invasor pode interceptar a comunicação entre o usuário e o servidor.

Figura 4 – Arquitetura Man-in-the-Middle Comum




*Fonte: (MELAMED, 2018)*

#### 2.5.2.4 Falhas na Gestão de Chaves e Certificados

A gestão inadequada de chaves criptográficas e certificados digitais pode levar a sérios problemas de segurança. O armazenamento inadequado de chaves privadas, a falta de rotação regular de chaves e a gestão incorreta de certificados podem comprometer a segurança de documentos digitais (DORNELES; CORRÊA, 2013). É fundamental adotar práticas recomendadas de segurança, como o uso de hardware seguro para armazenamento de chaves e a validação periódica de certificados, para garantir a proteção adequada dos elementos críticos. Para o contexto relativo ao aplicativo do presente trabalho, tais práticas se mostram determinantes e indispensáveis.

### 2.5.3 Medidas de Segurança em Aplicativos de Assinatura Digital

Para mitigar os riscos, várias medidas de segurança são implementadas em aplicativos de assinatura digital. Entre elas, destacam-se o uso de criptografia de ponta a ponta, autenticação multifator (MFA), e a validação de certificados digitais através de infraestruturas de chave pública (ICP) (COPALO, 2003; BARBOZA et al., 2018). Essas

técnicas garantem que apenas usuários autorizados possam acessar e assinar documentos, e que qualquer tentativa de adulteração seja facilmente detectável.

#### 2.5.3.1 Classificações de Segurança em Sistemas de Assinatura Digital

A segurança de sistemas computacionais pode ser classificada em diferentes níveis de acordo com critérios estabelecidos por padrões internacionais. Dentre esses, destaca-se o TCSEC (Trusted Computer System Evaluation Criteria), que define categorias de segurança, como A1, B1, B2, C1, entre outras. Cada nível estabelece requisitos específicos em termos de controle de acesso, auditoria e integridade do sistema (CENTER, 1987).

No contexto de aplicativos de assinatura digital, a adoção de níveis mais rigorosos de segurança é essencial para garantir a proteção contra acessos não autorizados e tentativas de adulteração. Segundo Center (1987), sistemas classificados no nível A1 possuem verificação formal de segurança e controles rigorosos para integridade e autenticação. Já os níveis B1 e B2 incluem mecanismos avançados de proteção, como listas de controle de acesso obrigatórias e auditoria detalhada de eventos, aumentando a confiabilidade dos processos de assinatura digital.

A Tabela 1 apresenta um resumo dos principais níveis de segurança estabelecidos pelo TCSEC e suas características:

Tabela 1 – Principais Níveis de Segurança Segundo o TCSEC

| **Nível** | **Descrição** |
|---|---|
| **A1** | Possui verificação formal de segurança, com rigorosos controles para integridade, autenticação e auditoria. Exige documentação detalhada e testes rigorosos do sistema. |
| **B1** | Implementa controle de acesso obrigatório e políticas de segurança bem definidas. Inclui auditoria de eventos e separação de usuários com diferentes níveis de acesso. |
| **B2** | Amplia os controles do nível B1, adicionando mecanismos mais robustos de proteção contra ameaças internas e externas, além de maior resistência a vulnerabilidades. |
| **C1** | Oferece controle de acesso básico, garantindo a separação entre usuários e seus respectivos arquivos, mas sem mecanismos avançados de auditoria ou proteção obrigatória. |
| **C2** | Expande o nível C1 ao adicionar registro de auditoria detalhado e mecanismos mais refinados de controle de acesso, melhorando a segurança contra acessos não autorizados. |

### 2.5.4 Confiabilidade de Aplicativos de Assinatura Digital

A confiabilidade de um aplicativo de assinatura digital depende tanto de sua robustez contra falhas quanto de sua capacidade de manter a integridade dos dados ao longo do tempo (CALÇADO, 2007). Testes rigorosos de segurança, auditorias regulares, e a conformidade com normas internacionais, como a eIDAS (Electronic Identification, Authentication and Trust Services), são práticas recomendadas para garantir que um sistema seja confiável e, portanto, bem visto entre os usuários, nacional ou internacionalmente (BERNARDO; KON, 2008; HÜHNLEIN, 2014; SANTOS, 2014).

#### 2.5.4.1 Princípio do Não Repúdio

O princípio do não repúdio assegura que o autor de uma assinatura digital não possa negar a autenticidade do documento assinado, sendo, portanto, essencial para garantir a validade jurídica das assinaturas eletrônicas. A criptografia assimétrica e os certificados digitais, emitidos por autoridades certificadoras confiáveis, vinculam cada assinatura de forma única ao seu signatário (MENKE, 2003).

Quando um documento assinado digitalmente é recebido, a verificação é feita por meio da chave pública do certificado digital, o que assegura tanto a validade da assinatura quanto a não revogação do certificado. Se a verificação for bem-sucedida, presume-se que o documento é autêntico e possui sua integridade mantida.

## 2.6 Integração em Aplicativos Mobile

### 2.6.1 Desafios da Integração de Serviços em Aplicativos Mobile

A integração de serviços em aplicativos mobile, especialmente aqueles que envolvem assinaturas digitais, apresenta desafios únicos. Isso inclui a compatibilidade com múltiplas plataformas (iOS e Android), a gestão de diferentes versões de API, e a manutenção da performance e segurança durante a integração (BIØRN-HANSEN; GRØNLI; GHINEA, 2018; FLORA; WANG; CHANDE, 2014). Um dos maiores desafios é garantir que a experiência do usuário seja consistente, independentemente do dispositivo ou sistema operacional utilizado.

### 2.6.2 Estratégias para uma Integração Eficiente

Para garantir uma integração eficiente, é essencial adotar boas práticas como o uso de APIs RESTful, serviços em nuvem e a arquitetura de microsserviços. Essas abordagens permitem uma maior flexibilidade e escalabilidade, facilitando a integração de novas funcionalidades e a comunicação entre diferentes serviços (AZEVEDO, 2020). Além disso, o

uso de contêineres (como Docker) pode ajudar a isolar ambientes de desenvolvimento e produção, minimizando conflitos de dependências (COMBE; MARTIN; PIETRO, 2016).

### 2.6.3 Integração com Sistemas Legados e Outras Plataformas

A integração com sistemas legados é um desafio comum em aplicativos de assinatura digital, especialmente em ambientes corporativos. Conforme exposto em Espindola, Majdenbaum e Audy (2004), é necessário garantir que o novo sistema possa se comunicar de forma eficaz com plataformas existentes, sem comprometer a integridade dos dados ou a segurança. O uso de intermediários de integração, como ESBs (Enterprise Service Buses), pode facilitar essa comunicação e reduzir a complexidade da integração (AZIZ et al., 2020).

## 2.7 Experiência do Usuário (UX)

A otimização da experiência do usuário (UX) em um aplicativo de assinatura digital é crucial para garantir interações eficientes e seguras. Segundo Brown (2021), a UX não se restringe apenas à interface, mas abrange todos os aspectos do uso, incluindo a facilidade de navegação e a eficiência do fluxo de trabalho.

### 2.7.1 Facilidade de Uso e Acessibilidade

Um dos aspectos mais críticos da UX em aplicativos de assinatura digital é a facilidade de uso. Usuários precisam ser capazes de navegar pelo aplicativo de forma intuitiva, sem necessidade de treinamento extenso. Isso inclui a simplificação dos processos de assinatura, onde o usuário pode rapidamente carregar um documento, adicionar uma assinatura digital e enviar o documento assinado, tudo em poucos passos. Nielsen (2020) enfatiza que uma interface limpa e minimalista pode reduzir a carga cognitiva, permitindo que os usuários se concentrem nas tarefas essenciais.

### 2.7.2 Integração com Outros Sistemas e Fluxos de Trabalho

Um aplicativo de assinatura digital deve ser facilmente integrável com outros sistemas e fluxos de trabalho já existentes. Isso significa que o aplicativo deve permitir a importação e exportação de documentos de diferentes plataformas, como armazenamento em nuvem, sistemas de gerenciamento de documentos (DMS), e softwares de e-mail. De acordo com Jones (2019), a integração com outros sistemas reduz a necessidade de processos manuais, melhorando a eficiência e reduzindo o risco de erro humano.

A integração perfeita com outros sistemas também facilita a incorporação da assinatura digital em processos de negócios existentes, como a aprovação de contratos ou a validação de documentos legais, sem interromper o fluxo de trabalho do usuário.

### 2.7.3 Facilidade de Uso e Acessibilidade

O feedback instantâneo durante o uso do aplicativo é outro elemento crucial. Informações como "documento assinado com sucesso" ou "erro na assinatura" devem ser fornecidas imediatamente para garantir que os usuários estejam sempre cientes do status de suas ações. Nielsen (2020) destaca que mensagens de erro claras e soluções sugeridas ajudam a minimizar a frustração e a melhorar a experiência geral do usuário.

Além disso, a inclusão de tutoriais interativos ou uma seção de ajuda abrangente pode auxiliar os usuários a se familiarizarem rapidamente com o aplicativo. Suporte ao usuário, seja via chat ao vivo ou através de FAQs bem estruturados, pode resolver dúvidas e problemas de forma eficiente, contribuindo para uma experiência positiva.

## 2.8 Usabilidade

A usabilidade é um conceito central na concepção de aplicativos, garantindo que o usuário consiga concluir suas tarefas de maneira rápida e sem confusão. No contexto de um aplicativo de assinatura digital, isso implica na organização clara das funções e na apresentação das informações de forma que o usuário compreenda o processo sem esforço excessivo (SHNEIDERMAN, 2016).

### 2.8.1 Simplificação do Processo de Assinatura

Em um aplicativo de assinatura digital, a usabilidade começa com a simplificação do processo de assinatura. Isso significa que as etapas para carregar, assinar e enviar um documento devem ser reduzidas ao mínimo necessário, sem comprometer a segurança. De acordo com Krug (2013), quanto menos passos o usuário precisar realizar, menor será a chance de confusão ou erros. Por exemplo, a implementação de uma função "arrastar e soltar" para adicionar documentos e uma barra de progresso visível durante o processo de assinatura pode aumentar significativamente a eficiência e clareza do processo.

### 2.8.2 Design Intuitivo de Interface

O design da interface de um aplicativo de assinatura digital deve ser intuitivo, com botões e menus claramente rotulados e organizados de maneira lógica. Segundo Norman (2013), a previsibilidade do comportamento da interface ajuda os usuários a se sentirem no controle, reduzindo a curva de aprendizado e aumentando a confiança no uso do aplicativo.

Ícones e atalhos que seguem convenções familiares, como ícones de lápis para edição ou cadeados para segurança, podem facilitar a navegação e garantir que o usuário compreenda instantaneamente a função de cada elemento da interface.

## 2.9 Acessibilidade

Garantir a acessibilidade em um aplicativo de assinatura digital significa assegurar que pessoas com diferentes tipos de limitações possam utilizar o sistema de forma autônoma. Isso inclui a adaptação da interface para usuários com deficiência visual, auditiva ou motora, além de considerar diferentes contextos de uso, como dispositivos móveis com variações de tamanho de tela.

### 2.9.1 Design Inclusivo e Suporte a Tecnologias Assistivas

O design inclusivo é uma abordagem essencial para garantir que o aplicativo de assinatura digital seja acessível a todos. Isso inclui a implementação de recursos que permitam o uso do aplicativo por pessoas com diferentes necessidades, como a compatibilidade com tecnologias assistivas. De acordo com a Web Accessibility Initiative (WAI) (WAI) (2018), o suporte a leitores de tela, como o JAWS ou o NVDA, é fundamental para garantir que pessoas com deficiência visual possam navegar e utilizar o aplicativo sem barreiras. Além disso, o uso de textos alternativos descritivos para imagens e ícones ajuda a transmitir informações visuais de forma acessível.

### 2.9.2 Contraste de Cores e Legibilidade

Para garantir a acessibilidade, é vital que o aplicativo ofereça opções de contraste de cores adequadas, especialmente para usuários com daltonismo ou outras deficiências visuais. Segundo Smith (2020), o contraste de cores entre o texto e o fundo deve atender aos padrões estabelecidos para legibilidade, como o contraste mínimo de 4,5:1 recomendado pelo WCAG. Isso garante que o texto seja facilmente legível em qualquer condição, evitando o cansaço visual e aumentando a usabilidade geral.

Além do contraste, o tamanho e a clareza da fonte também são críticos. O aplicativo deve permitir ajustes de tamanho de fonte e oferecer fontes claras e sem serifa para melhorar a legibilidade, especialmente em dispositivos móveis. Isso é particularmente importante em um aplicativo de assinatura digital, onde a precisão na leitura e compreensão dos termos e condições é essencial.

## 2.10 Considerações Finais do Capítulo

Neste capítulo, foi discutida a base teórica necessária para o desenvolvimento do aplicativo mobile de assinatura digital. Foram apresentados os conceitos de Documentos Digitais e Assinatura Digital, com destaque para os Certificados Digitais e a ICP-Brasil. Também se exploraram os Padrões e Protocolos de Segurança e os Aspectos Legais, enfatizando a Validade Jurídica das assinaturas digitais no Brasil.

Além disso, abordou-se a Segurança e Confiabilidade em aplicativos de assinatura digital, analisando as principais ameaças e medidas de segurança. A Integração em Aplicativos Mobile foi discutida, incluindo os desafios e estratégias para garantir uma integração eficiente com outras plataformas. Por fim, aspectos de Experiência do Usuário (UX), Usabilidade e Acessibilidade foram destacados como essenciais para o sucesso do aplicativo.

# 3 Suporte Tecnológico

Neste capítulo, são abordados os principais recursos tecnológicos que viabilizaram este trabalho. Como o trabalho envolveu a implementação de assinaturas digitais em aplicativos mobile, há necessidade de ferramentas que permitissem desde a modelagem e prototipação das interfaces, até ferramentas específicas de desenvolvimento e gerenciamento de versões. Tais ferramentas são apresentadas em detalhes mais adiante, respectivamente organizadas nas seções: Ferramentas de Modelagem; Ferramentas de Desenvolvimento ; e Ferramentas de Gerenciamento.

Adicionalmente, foram utilizadas ferramentas que apoiaram em diferentes demandas (ex. teste de APIs, autenticação de usuários e documentação técnica), sendo as principais reveladas na seção Ferramentas Auxiliares. Por fim, tem-se o Resumo do Capítulo.

## 3.1 Ferramentas de Modelagem

### 3.1.1 Figma

O Figma é uma ferramenta de design colaborativo baseada em nuvem que permite aos usuários e desenvolvedores criarem interfaces de usuário, protótipos e wireframes de forma colaborativa Figma (2022). Esta plataforma é amplamente utilizada por designers e equipes de desenvolvimento devido às suas diversas funcionalidades que facilitam a criação e a prototipação de interfaces.

### 3.1.2 Draw.io

Draw.io é uma ferramenta de diagramação que permite criar diagramas de fluxo e modelos de processos. É especialmente útil para mapear os fluxos de trabalho e a arquitetura de sistemas de assinatura digital (JGRAPH LTD., 2022).

### 3.1.3 LucidChart

LucidChart é uma ferramenta de modelagem visual que facilita a criação de diagramas e fluxos de trabalho, colaborando em tempo real com outros membros da equipe. É excelente para criar diagramas de arquitetura de software e fluxos de dados (LUCID SOFTWARE INC., 2022).

### 3.1.4 Bizagi Modeler

O Bizagi Modeler é uma ferramenta robusta de modelagem de processos de negócios que permite a criação de diagramas de fluxo de trabalho e processos de negócios. Ele facilita a visualização e análise de processos, sendo amplamente utilizado para mapear fluxos de atividades e otimizar a compreensão de processos complexos (MODELER, 2024). No contexto deste trabalho, o Bizagi foi utilizado para representar visualmente os fluxos de atividades relacionados ao processo de assinatura digital e metodologias associadas ao desenvolvimento do projeto.

## 3.2 Ferramentas de Desenvolvimento

### 3.2.1 OpenSSL

OpenSSL é uma biblioteca robusta de ferramentas de criptografia que permite a implementação de protocolos de segurança, como SSL e TLS, além de oferecer suporte para a criação e verificação de assinaturas digitais (THE OPENSSL PROJECT, 2022).

### 3.2.2 React Native

React Native é uma biblioteca de desenvolvimento de aplicativos móveis que permite criar aplicativos para iOS e Android usando JavaScript. Pode ser utilizada para desenvolver interfaces de usuário para aplicativos de assinatura digital (React Native, 2022).

### 3.2.3 Java

Java é uma linguagem de programação amplamente utilizada no desenvolvimento Android, destacando-se por sua robustez, portabilidade e extensa comunidade de suporte. Sua execução baseada em máquina virtual permite rodar o mesmo código em diferentes dispositivos, enquanto sua vasta coleção de bibliotecas e frameworks facilita a criação de soluções complexas. Apesar de sua sintaxe mais longa, Java é uma escolha confiável e bem integrada à plataforma Android (ORACLE, 2024).

### 3.2.4 Kotlin

Kotlin é uma linguagem moderna e oficial para o desenvolvimento Android, reconhecida por sua sintaxe concisa e recursos avançados, como tratamento nativo de nulidade e coroutines para programação assíncrona. Totalmente interoperável com Java, Kotlin prioriza produtividade e segurança, sendo a escolha ideal para novos projetos por simplificar tanto o desenvolvimento quanto a manutenção (KOTLIN, 2024).

### 3.2.5 Python

Python é uma linguagem de alto nível conhecida por sua simplicidade e facilidade de uso, sendo amplamente aplicada em áreas como análise de dados, aprendizado de máquina e desenvolvimento web. Embora não seja nativa para o desenvolvimento Android, Python pode ser usado em scripts auxiliares, automação e, com ferramentas específicas, no desenvolvimento de aplicativos móveis (PYTHON, 2024).

### 3.2.6 FastAPI

FastAPI é um framework web moderno e de alta performance para a construção de APIs em Python, utilizando tipagem automática para validações rápidas e robustas. Baseado no Starlette para a camada de rede e no Pydantic para validação de dados, o FastAPI é conhecido por sua rapidez e simplicidade de uso. Ele suporta assincronismo nativo (async/await), o que permite a construção de APIs altamente escaláveis e responsivas (FastAPI, 2022).

### 3.2.7 PostgreSQL

PostgreSQL é um sistema de gerenciamento de banco de dados relacional de código aberto conhecido por sua robustez, extensibilidade e conformidade com o padrão SQL. Ele oferece suporte avançado para consultas complexas, integridade de dados e desempenho otimizado. No contexto deste trabalho, o PostgreSQL é utilizado para armazenar informações relacionadas às assinaturas digitais e usuários, garantindo segurança e escalabilidade (PostgreeSQL, 2024).

### 3.2.8 AWS EC2

Amazon Elastic Compute Cloud (EC2) é um serviço de computação em nuvem que fornece capacidade de processamento escalável na AWS. Com instâncias personalizáveis, ele permite hospedar e gerenciar servidores virtuais, suportando a implantação de aplicativos de forma flexível e segura. No contexto deste projeto, o AWS EC2 é utilizado para hospedar a aplicação AssinApp, garantindo alta disponibilidade e desempenho (AWS, 2024).

## 3.3 Ferramentas de Gerenciamento

### 3.3.1 Git e GitHub

Git é um sistema de controle de versão distribuído, enquanto o GitHub é uma plataforma baseada na web que utiliza Git. Eles são essenciais para o gerenciamento de

código fonte e colaboração entre equipes de desenvolvimento (Git, 2022; GitHub, 2022).

### 3.3.2 Jira

Jira é uma ferramenta de gerenciamento de projetos que ajuda a rastrear problemas, tarefas e progresso do desenvolvimento de software. É útil para coordenar as atividades de desenvolvimento de um aplicativo de assinatura digital (Jira, 2022).

## 3.4 Ferramentas Auxiliares

### 3.4.1 Android Studio

O Android Studio é o ambiente integrado de desenvolvimento (IDE) oficial para criar aplicativos na plataforma Android. Ele fornece um conjunto completo de ferramentas avançadas, incluindo editores visuais de layout, emuladores para testes e compatibilidade com linguagens como Java e Kotlin, facilitando o desenvolvimento, a análise e a depuração de aplicativos (ANDROID, 2024).

### 3.4.2 Docker

Docker é uma plataforma que possibilita a criação, gestão e execução de aplicativos em contêineres, oferecendo ambientes isolados e consistentes. Ela facilita o desenvolvimento e a implantação ao agrupar dependências e configurações em contêineres portáteis. No contexto de validação de assinaturas digitais, Docker pode ser usado para rodar APIs, simular ambientes de produção e automatizar testes (DOCKER, 2020).

### 3.4.3 React Native PDF

React Native PDF é uma biblioteca para React Native que facilita a exibição e manipulação de arquivos PDF em dispositivos móveis. Com recursos como navegação, zoom e personalização de renderização, ela permite integrar visualizações de documentos PDF de forma prática. No contexto de assinaturas digitais, essa biblioteca pode ser utilizada para abrir e interagir com documentos assinados diretamente no aplicativo (REACT NATIVE, 2024).

### 3.4.4 Expo

Expo é uma ferramenta e plataforma que simplifica o desenvolvimento de aplicativos React Native, oferecendo um conjunto de ferramentas que facilitam a construção, publicação e manutenção de aplicativos móveis (Expo, 2022).

### 3.4.5 Expo Document Picker

A API Expo Document Picker permite aos usuários selecionar arquivos diretamente de seus dispositivos, suportando uma ampla variedade de formatos. Essa funcionalidade é especialmente útil para implementar uploads ou interações com documentos em aplicativos móveis. No contexto de assinaturas digitais, a ferramenta pode ser aplicada para importar arquivos que serão assinados ou verificados no aplicativo (EXPO, 2024).

### 3.4.6 JSON Web Token (JWT)

JSON Web Token (JWT) é um padrão aberto que permite a troca segura de informações entre diferentes partes por meio de objetos JSON compactos e criptograficamente assinados. Um JWT é dividido em três partes principais: cabeçalho, payload e assinatura, garantindo tanto a integridade quanto a autenticidade dos dados. Amplamente utilizado em autenticação e autorização, ele assegura o acesso seguro a recursos protegidos. No contexto de assinaturas digitais, o JWT pode ser empregado para validar a identidade de usuários e proteger operações, como assinaturas e validações de documentos (NPM, 2024).

### 3.4.7 Overleaf e LaTeX

Overleaf é uma plataforma colaborativa para escrever, editar e publicar documentos científicos em LaTeX. É útil para a documentação técnica do projeto, permitindo a criação de relatórios detalhados e bem formatados (Overleaf, 2022).

## 3.5 Considerações Finais do Capítulo

Neste capítulo, foram exploradas diversas ferramentas essenciais para o desenvolvimento, prototipagem, criptografia e gerenciamento de projetos de software. Foram abordadas ferramentas de design colaborativo como o Figma, ferramentas de diagramação como Draw.io e LucidChart, e ferramentas de desenvolvimento como OpenSSL, Bouncy Castle, Node.js, React Native e Expo. Além disso, foram discutidas ferramentas de gerenciamento como Git, GitHub e Jira, e ferramentas auxiliares como Postman, Firebase, Overleaf e LaTeX. Cada uma dessas ferramentas desempenha um papel crucial nas diferentes fases do ciclo de vida do desenvolvimento de software, desde a concepção do design até a implementação e teste.

A seguir, apresenta-se o quadro resumo detalhado na Tabela 2, que mostra o nome, descrição e links para as principais ferramentas discutidas neste capítulo.

Tabela 2 – Resumo das ferramentas

| **Nome** | **Descrição** | **Link** |
|---|---|---|
| Figma | Ferramenta de design colaborativo. | <https://www.figma.com> |
| Draw.io | Ferramenta de diagramação para criar fluxos. | <https://www.draw.io> |
| LucidChart | Ferramenta de modelagem visual. | <https://www.lucidchart.com> |
| Bizagi Modeler | Ferramenta de modelagem de processos de negócios. | <https://www.bizagi.com/pt-br/products/bpm-suite/modeler> |
| OpenSSL | Biblioteca de criptografia robusta. | <https://www.openssl.org> |
| React Native | Framework para criação de aplicativos nativos. | <https://reactnative.dev> |
| Expo | Plataforma para desenvolvimento de aplicativos React Native. | <https://expo.dev> |
| Expo Document Picker | API para seleção de arquivos nos dispositivos. | <https://docs.expo.dev/versions/latest/sdk/document-picker/> |
| React Native PDF | Biblioteca para exibição e manipulação de PDFs em dispositivos móveis. | <https://github.com/wonday/react-native-pdf> |
| Git | Sistema de controle de versão distribuído. | <https://git-scm.com> |
| GitHub | Plataforma para hospedagem e gerenciamento de repositórios Git. | <https://github.com> |
| Jira | Ferramenta de gerenciamento de projetos e tarefas. | <https://www.atlassian.com/software/jira> |
| Docker | Plataforma para criar e executar aplicativos em contêineres. | <https://www.docker.com> |
| JSON Web Token (JWT) | Padrão para troca segura de informações por meio de tokens. | <https://jwt.io> |

| Continuação da Tabela | | |
|---|---|---|
| Android Studio | IDE oficial para desenvolvimento de aplicativos Android. | <https://developer.android.com/studio> |
| Java | Linguagem de programação robusta para desenvolvimento Android. | <https://www.oracle.com/java/> |
| Kotlin | Linguagem moderna para desenvolvimento Android. | <https://kotlinlang.org> |
| Python | Linguagem versátil para scripts auxiliares e automação. | <https://www.python.org> |
| FastAPI | Framework moderno para desenvolvimento de APIs de alto desempenho com Python. | <https://fastapi.tiangolo.com> |
| Overleaf | Plataforma colaborativa para edição de documentos LaTeX. | <https://www.overleaf.com> |
| LaTeX | Sistema de preparação de documentos, especialmente para a escrita científica e técnica. | <https://www.latex-project.org> |
| PostgreSQL | Sistema de gerenciamento de banco de dados relacional e objeto, conhecido por sua robustez e conformidade com padrões SQL. | <https://www.postgresql.org> |
| AWS EC2 | Serviço de computação em nuvem que oferece capacidade de processamento escalável na nuvem. Utilizado para hospedagem de aplicações e ambientes de desenvolvimento. | <https://aws.amazon.com/ec2> |

# 4 Metodologia

## 4.1 Classificação da Pesquisa

Objetivando a obtenção de respostas cientificamente fundamentadas para problemas propostos, a pesquisa científica atua como o principal elemento de apoio ao conhecimento, tanto em nível teórico quanto prático. Conforme exposto em Gerhardt e Silveira (2009), os elementos de pesquisa são elencados e classificados quanto à **abordagem**, **natureza**, **objetivos** e **procedimentos**.

A presente seção apresenta os tipos de pesquisa que forneceram suporte para o desenvolvimento do trabalho, com base na classificação antes mencionada, destacando como cada tipo contribuiu para os diferentes aspectos do estudo.

### 4.1.1 Abordagem

No que diz respeito à abordagem, o presente trabalho pôde ser classificado como uma pesquisa com abordagem mista, combinando métodos **quantitativos** e **qualitativos**. Segundo Gerhardt e Silveira (2009), a pesquisa quantitativa pauta-se na objetividade e no positivismo, analisando dados brutos como ferramenta essencial para a compreensão da realidade. Já a pesquisa qualitativa busca interpretar fenômenos a partir das percepções e experiências dos indivíduos, permitindo uma compreensão mais ampla e subjetiva dos resultados.

Dessa forma, a avaliação do aplicativo AssinApp foi realizada por meio da análise de métricas quantitativas, como desempenho do sistema, tempo médio para assinatura e taxa de sucesso na execução das tarefas. Além disso, a pesquisa qualitativa foi conduzida através de questionários, permitindo coletar percepções dos usuários sobre a usabilidade e a experiência com a aplicação.

### 4.1.2 Natureza

Relativo à natureza, a pesquisa pôde ser classificada como **aplicada**. A pesquisa aplicada busca promover saberes voltados para a aplicação prática, orientada à resolução de problemas específicos. Em contrapartida, a pesquisa básica visa gerar conhecimentos para o avanço da ciência, sem focar, portanto, na aplicação prática desses saberes (GERHARDT; SILVEIRA, 2009).

Essa definição está diretamente relacionada ao objetivo do presente trabalho, que destinou-se a utilizar os conhecimentos adquiridos como base para a implementação de

uma aplicação que seja condizente com o contexto da prática da assinatura digital no Brasil.

### 4.1.3 Objetivos

Quanto aos objetivos, a presente pesquisa pôde ser classificada como **exploratória**. Este tipo de pesquisa proporciona maior familiarização com o problema, com o intuito de explicitar o problema e promover subsídios para a criação de hipóteses. Seu planejamento é, desta forma, marcado pela flexibilidade, de modo a levar em consideração variados aspectos relativos ao fato estudado, e pode envolver etapas como levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e análise de exemplos que "estimulem a compreensão" dos fenômenos estudados (GIL, 2002).

### 4.1.4 Procedimentos

Com relação aos procedimentos, dois tipos principais puderam ser elencados como elementos de apoio para a realização do presente trabalho ao longo de suas etapas: a **pesquisa bibliográfica** e a **pesquisa-ação**.

A pesquisa bibliográfica se dá através do levantamento de referências teóricas anteriormente analisadas e disseminadas por meio de artefatos escritos manual ou eletronicamente, como livros, artigos científicos, páginas web, entre outros. Deste modo, um trabalho científico inicia-se com a pesquisa bibliográfica, com vistas a fornecer ao pesquisador um arcabouço intelectual interessante vinculado aos estudos anteriormente realizados sobre o assunto (FONSECA, 2002).

Por outro lado, a pesquisa-ação se diferencia ao envolver a participação ativa do pesquisador no processo de investigação e intervenção. Conforme descrito em Thiollent (2022), este tipo de pesquisa é caracterizado por ser uma investigação social de viés empírico, que possui sua concepção e realização atreladas a uma ação ou resolução de um problema coletivo. Desta forma, os pesquisadores e representantes participativos atuam de modo cooperativo, com vistas à realização de tais ações.

## 4.2 Metodologia de Pesquisa Bibliográfica

A pesquisa bibliográfica foi desenvolvida com base em materiais previamente elaborados, incluindo livros e artigos científicos. Este tipo de pesquisa é fundamental para consolidar o entendimento do tema e sustentar teoricamente o trabalho desenvolvido.

### 4.2.1 String de Busca

Para o levantamento bibliográfico, foi definido o tema de pesquisa e, a partir disso, elaborou-se uma string de busca que pudesse retornar materiais relevantes. O refinamento da string de busca foi realizado para garantir resultados consistentes e adequados ao tema. As principais plataformas utilizadas foram:

- **Google Acadêmico**[1]: Ferramenta utilizada para identificar artigos científicos de relevância para o tema;
- **Biblioteca Digital da Produção Intelectual Discente - UnB**[2]: Utilizada para a consolidação do processo de entendimento do tema, permitindo acesso a trabalhos acadêmicos já realizados e alinhados ao escopo desta pesquisa.

A Tabela 3, a seguir, apresenta a elaboração da string de busca, o refinamento realizado e as respectivas bases de dados utilizadas.

Tabela 3 – Elaboração da String de Busca

| **String** | **Base de Dados** | **Quantidade** |
|---|---|---|
| "assinatura digital"AND "criptografia" | Google Acadêmico | 9240 |
| "assinatura digital"AND "criptografia" | Biblioteca Digital da UnB | 19433 |
| "certificado digital"AND "validação" | Google Acadêmico | 34900 |
| "certificado digital"AND "validação" | Biblioteca Digital da UnB | 19518 |
| "assinatura eletrônica"AND "validade jurídica" | Google Acadêmico | 17000 |
| "assinatura eletrônica"AND "validade jurídica" | Biblioteca Digital da UnB | 3265 |

*Fonte: Autor*

### 4.2.2 Critérios de Seleção

Para selecionar os materiais mais relevantes, foram definidos critérios claros de inclusão e exclusão, utilizando-se da leitura exploratória, conforme estabelecido em Gil (2002). Esta etapa consistiu na análise de títulos, resumos e palavras-chave. Os critérios estabelecidos foram:

- Relacionar-se ao tema de assinatura digital ou certificação digital;
- Abordar aspectos legais e de segurança associados ao contexto do projeto;
- Ter publicação em fontes confiáveis e de relevância acadêmica.

[1] Disponível em: <https://scholar.google.com.br/>. Acesso em: 28 jan. 2025.
[2] Disponível em: <https://bdm.unb.br/>. Acesso em: 28 jan. 2025.

Com base nesses critérios, foi formada uma base de artigos e livros que embasaram o presente trabalho, sendo os seguintes materiais selecionados como mais aderentes ao tema:

- *Planning for PKI: best practices guide for deploying public key infrastructure* (2001a);
- *Assinatura Eletrônica GOV.BR* (2022);
- *Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers issuing certificates; Part 1: General requirements* (2012);
- *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures* (1999);
- *Market Guide for Digital Signature Solutions* (2023);
- *Digital signature standard (DSS)* (2000);
- *ETSI Digital Signature Standard* (2012);
- *Criptografia e segurança de redes: Princípios e práticas* (2006);

Por meio do **Google Acadêmico**, foi possível organizar e rastrear os materiais mais relevantes, garantindo o suporte adequado para a fundamentação teórica apresentada no *Capítulo 2* e a estruturação desta pesquisa.

## 4.3 Metodologia de Desenvolvimento

O desenvolvimento do projeto foi orientado por uma combinação das metodologias ágeis **Kanban**, **Scrum** e **XP**, permitindo maior flexibilidade e entregas incrementais ao longo do processo. Essas abordagens foram escolhidas devido à sua capacidade de se adaptar rapidamente às mudanças e à constante evolução das necessidades do projeto.

**Kanban** é um método visual que utiliza um quadro para gerenciar as diferentes fases do processo de desenvolvimento. Ele não possui papéis ou artefatos definidos, como o Scrum, e não trabalha com sprints. Seus princípios incluem a visualização do fluxo de trabalho, a limitação do trabalho em andamento, revisões periódicas dos entregáveis e a busca pela melhoria contínua (BOEG, 2010).

Por outro lado, o **Scrum** é um framework que define papéis específicos, como Scrum Master, time e Dono do Produto, e organiza o trabalho em sprints. O Scrum permite uma gestão clara das entregas, com um backlog de produto que organiza e prioriza os requisitos de desenvolvimento (SCHWABER; SUTHERLAND, 2011). No contexto deste

projeto, foram seguidas algumas práticas do Scrum, como o planejamento interativo, a colaboração constante, entregas incrementais, decisões empíricas e autogerenciamento.

Além disso, também foi utilizada uma abordagem de **XP** (Extreme Programming), que enfatiza a programação em pares, a refatoração constante do código e o feedback contínuo, conforme elencado em Fadel e Silveira (2010). Essas práticas contribuíram para um desenvolvimento de alta qualidade, focado na entrega de valor ao usuário e na melhoria constante do sistema.

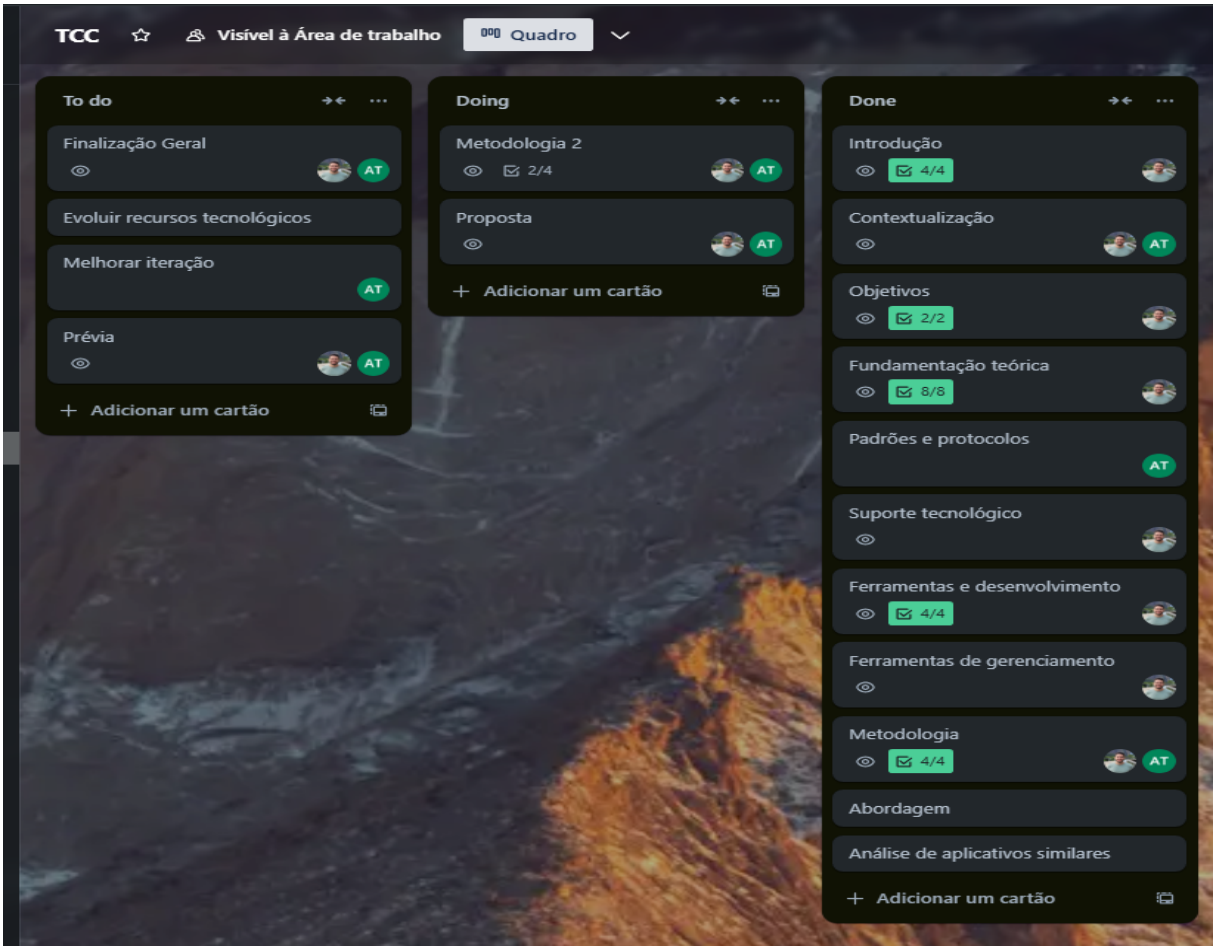
A combinação de Kanban, Scrum e XP foi fundamental para o andamento do projeto, aproveitando a flexibilidade do Kanban, a estrutura de backlog do Scrum e as boas práticas do XP.

O quadro Kanban foi implementado utilizando o Trello, como ilustrado na Figura 5, que facilitou o gerenciamento e a comunicação entre os membros da equipe. O Trello foi uma ferramenta crucial para garantir a visualização constante do progresso das tarefas, além de permitir a organização e a priorização das atividades de forma clara e eficiente.

Ao final de cada iteração, foram realizadas reuniões para revisar o progresso, avaliar a qualidade das entregas e planejar as próximas etapas. Isso garantiu que o desenvolvimento estivesse sempre alinhado com os objetivos e os requisitos do projeto.

Além disso, as releases regulares permitiram testar e validar as funcionalidades desenvolvidas, ajustando conforme o feedback recebido, e garantindo a qualidade e a relevância do produto.

Figura 5 – Processo de desenvolvimento Trello

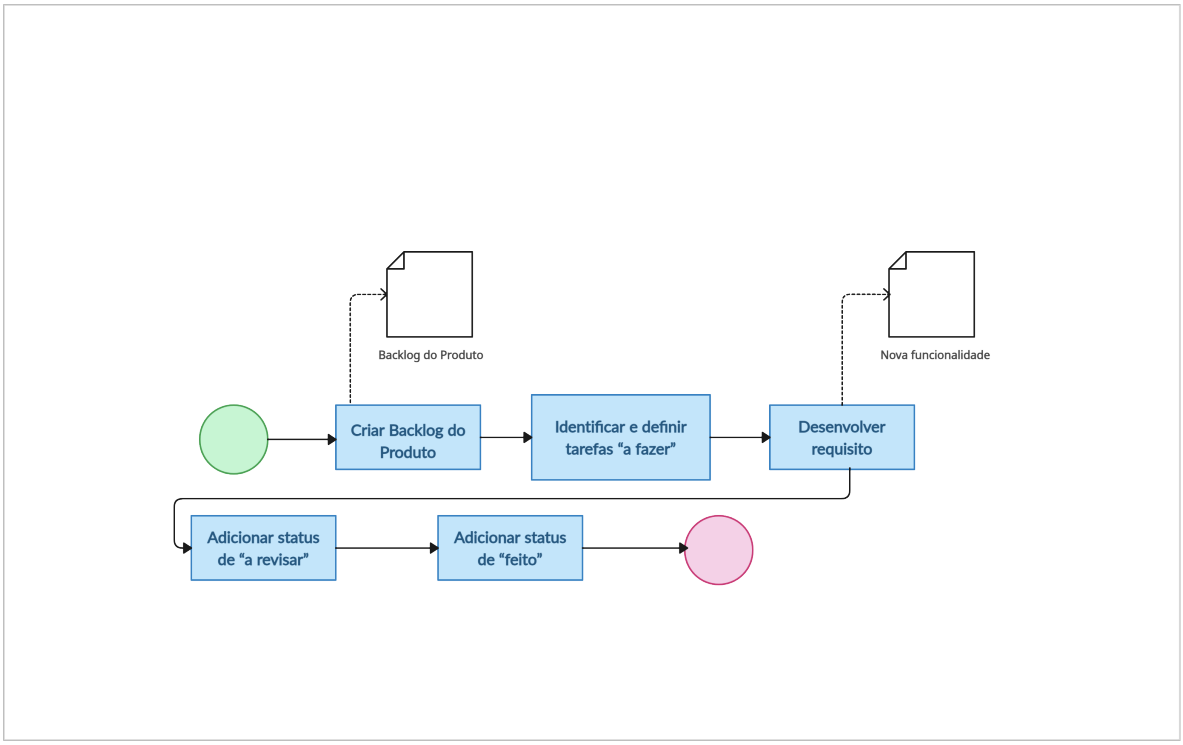



*Fonte: Autor*

A seguir, é apresentado o fluxo do processo de desenvolvimento, adaptado para o contexto deste TCC, conforme ilustrado na Figura 6.

- **Backlog do Produto**: lista de todos os requisitos e tarefas necessárias para a conclusão do TCC.
- **A Fazer**: tarefas priorizadas para desenvolvimento nas próximas iterações.
- **Em Progresso**: tarefas em desenvolvimento.
- **A Revisar**: tarefas concluídas, aguardando revisão e possíveis ajustes.
- **Feito**: tarefas finalizadas e prontas para integração ao sistema final.

Figura 6 – Processo de desenvolvimento da proposta do presente Trabalho de Conclusão de Curso




*Fonte: Autor*

## 4.4 Metodologia de Análise de Resultados

A análise dos resultados deste trabalho foi conduzida por meio da metodologia de pesquisa-ação. Segundo Thiollent (2022), a pesquisa-ação é uma abordagem interpretativa e empírica que envolve a identificação de um problema dentro de um contexto social e a implementação de ações para sua solução.

No contexto do AssinApp, a avaliação foi realizada sob duas perspectivas: qualitativa e quantitativa. De maneira qualitativa, analisou-se se o aplicativo atende às necessidades dos usuários em termos de desempenho, usabilidade e segurança da assinatura digital. De maneira quantitativa, foram considerados aspectos como o tempo de processamento das assinaturas digitais e a taxa de sucesso na validação de documentos.

A pesquisa-ação busca integrar pesquisa e prática, promovendo intervenções que resultem em melhorias contínuas no sistema. Conforme elenca Gil (2002), essa abordagem compreende diversas etapas, das quais foram adaptadas as seguintes para este trabalho:

- **Coleta de Dados:** a coleta de dados foi realizada por meio de testes práticos do aplicativo em diferentes cenários de uso, avaliando desde a experiência do usuário até a eficiência da validação das assinaturas digitais.

- **Análise e Interpretação dos Dados:** os dados coletados foram analisados empiricamente, verificando possíveis falhas, dificuldades enfrentadas pelos usuários e oportunidades de melhoria.
- **Elaboração do Plano de Ação:** com base na análise dos dados, foram planejadas melhorias para otimizar a usabilidade, a segurança e a eficiência do aplicativo, aproximando-o ainda mais das necessidades dos usuários.
- **Divulgação dos Resultados:** os resultados obtidos ao final do ciclo foram documentados, possibilitando a iteração contínua do desenvolvimento e a evolução do produto proposto.

## 4.5 Fluxo de Atividades

Com o intuito de conduzir as atividades, bem como os subprocessos a elas associados, foi elaborada uma modelagem referente ao fluxo de atividades. A Figura 7 ilustra o fluxograma, organizado em duas etapas as quais representaram as fases relativas ao projeto. Na sequência, constam as descrições de cada atividade e subprocesso:

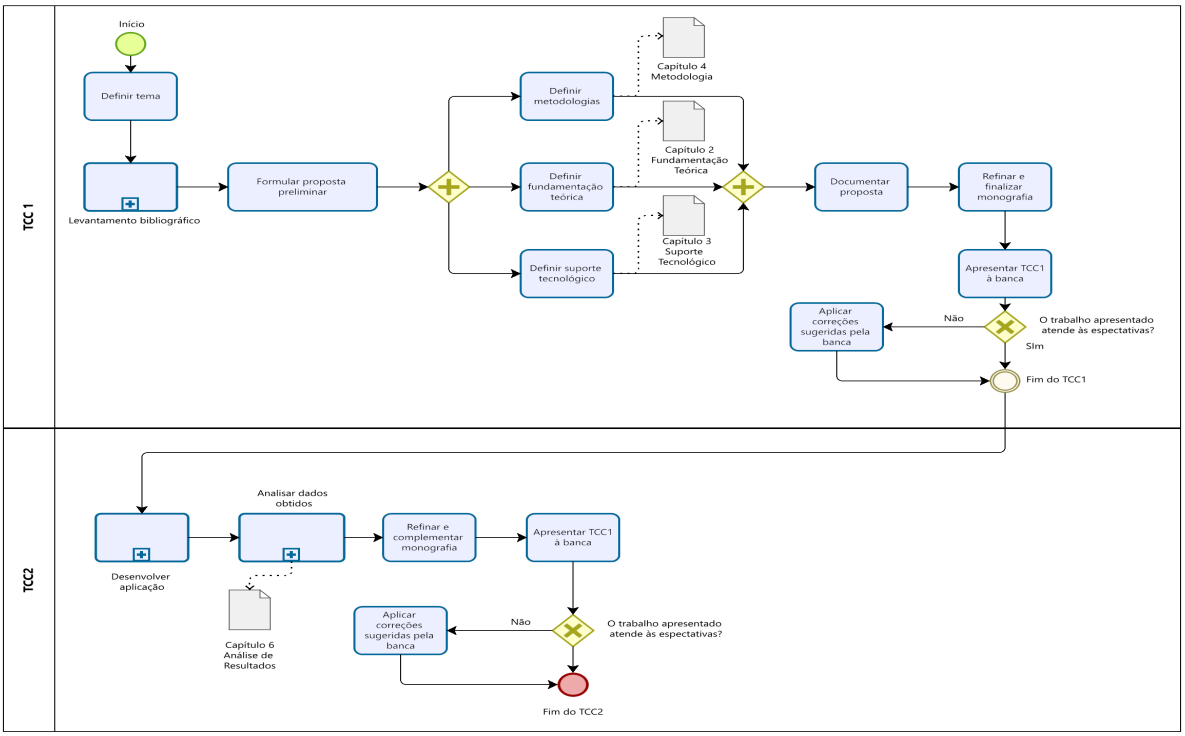
- **Definir Tema**: Executada juntamente com o orientador, consistiu na escolha do tema de interesse e afinidade do autor, e que, preferencialmente, pudesse resultar em uma hipótese a ser explorada. Desta forma, optou-se por pesquisar a respeito de soluções mobile associadas ao contexto de assinaturas digitais.
- **Levantamento Bibliográfico**: Subprocesso que compreendeu aglutinar materiais pertinentes sobre o tema e que pudessem, potencialmente, servir como suporte teórico para a realização da monografia. Tal atividade foi orientada pela metodologia de pesquisa bibliográfica descrita na seção 4.2 deste capítulo.
- **Formular Proposta Preliminar**: Definido o problema a ser solucionado, buscou-se apresentar uma proposta prática de solução através de capítulo, apresentando a Justificativa, as Questões de Pesquisa, e os Objetivos Gerais e Específicos.
- **Definir Referencial Teórico**: Estabeleceu-se o referencial teórico associado à prática de Assinatura Digital e aspectos correlatos como Criptografia Assimétrica, Algoritmos Criptográficos, Certificados Digitais, além de Padrões e Protocolos, Segurança e Confiabilidade, Ameaças e Vulnerabilidades, e Aspectos Legais e Jurídicos referentes à problemática. Esta atividade resultou no capítulo FUNDAMENTAÇÃO TEÓRICA.
- **Estabelecer Suporte Tecnológico**: Especificaram-se as tecnologias e ferramentas a serem utilizadas no desenvolvimento da proposta, bem como outros pormenores

associados à implementação da solução. Esta atividade resultou no capítulo SUPORTE TECNOLÓGICO.

- **Definir Metodologias**: Descreveu-se as metodologias e atividades de apoio aplicadas ao contexto do projeto, com o objetivo de fornecer orientações para os processos e subprocessos que compreendem o escopo do projeto em sua totalidade. Tal atividade encontra-se no presente capítulo.
- **Documentar Proposta**: Forneceu-se uma descrição detalhada de diferentes aspectos do aplicativo para apresentá-lo de maneira clara e objetiva. Dentre os elementos documentados estão a visão geral da arquitetura, a identidade visual e as funcionalidades do aplicativo.
- **Refinar Monografia**: Com um melhor entendimento acerca do tema, a partir da evolução decorrente das fases de pesquisa bibliográfica e definição do suporte tecnológico, realizou-se ajustes finais relativos à escrita e ao conteúdo associado ao tema, compreendendo tanto artefatos entregues como aspectos teóricos redigidos.
- **Apresentar à Banca**: Submeteu-se o texto à banca examinadora e realizou-se sua posterior apresentação para fins de avaliação.
- **Aplicar Correções Solicitadas pela Banca (Etapa Inicial)**:Foram aplicadas as correções sugeridas pela banca examinadora com base no que lhe foi apresentado, seja na apresentação oral ou na monografia entregue.
- **Desenvolvimento do Aplicativo**: subprocesso do projeto que envolveu a criação e a administração do código-fonte do aplicativo, seguindo as diretrizes da Metodologia de Desenvolvimento de Software. O objetivo foi criar um aplicativo que pudesse realizar a assinatura digital válida de documentos, objetivando maior segurança aos documentos digitais.
- **Análise de Resultados**: Subprocesso que encarregou-se de conduzir as atividades de pesquisa e validação, seguindo a Metodologia de Análise de Resultados. Este subprocesso foi cíclico, baseado em um protocolo de pesquisa adaptado e previamente estabelecido. O objetivo foi responder às seguintes perguntas de pesquisa: “Como desenvolver um aplicativo móvel eficaz para assinatura digital de documentos que garanta a integridade e a autenticidade das assinaturas?”, e “Quais métodos podem ser utilizados para validar assinaturas digitais e prevenir fraudes?”, além de alcançar os objetivos delineados no capítulo de introdução.
- **Refinar e Complementar Monografia**: Foram realizados os ajustes finais, em termos de escrita e elaboração de artefatos, procurando concluir a documentação do trabalho.

- **Apresentar à Banca**: A monografia foi entregue e o trabalho apresentado à Banca Examinadora.
- **Aplicar Correções Solicitadas pela Banca (Etapa Final)**: Aplicaram-se as correções sugeridas pela Banca Examinadora em relação ao que foi apresentado a ela.

Figura 7 – Processo de atividades do Trabalho de Conclusão de Curso




*Fonte: Autor*

## 4.6 Considerações Finais do Capítulo

Neste capítulo, foram abordadas as metodologias adotadas para o desenvolvimento do trabalho, detalhando a classificação da pesquisa, a abordagem metodológica e os procedimentos utilizados. Também foram explorados aspectos associados à metodologia investigativa e de análise dos resultados refrentes à pesquisa-ação.

Além disso, abordou-se a respeito da metodologia de desenvolvimento a qual envolveu o uso do Trello e da abordagem ágil iterativo-incremental, facilitando a gestão e o progresso do projeto. O fluxo de atividades também foi apresentado, permitindo um acompanhamento eficiente e a realização de ajustes conforme necessário.

# 5 AssinApp

Neste capítulo, é apresentado o aplicativo AssinApp, que foi desenvolvido no decorrer deste trabalho, visando facilitar a assinatura digital de documentos em um ambiente seguro e em conformidade com as normas brasileiras. Nesse sentido, na Contextualização, retoma-se a problemática e os desafios relacionados à autenticação e validação de documentos digitais. Posteriormente, na seção Estudo de soluções similares, são elencados outros aplicativos do segmento, por meio dos quais é possível estabelecer um comparativo. Adicionalmente, detalham-se Sobre o Aplicativo AssinApp, as Personas, os Requisitos, a Identidade Visual e a Arquitetura definida para o projeto. Por fim, são apresentadas as Considerações Finais do capítulo.

## 5.1 Contextualização

Com o avanço da digitalização e a crescente necessidade de processos eletrônicos seguros, a assinatura digital tornou-se uma ferramenta essencial para garantir a autenticidade e integridade dos documentos eletrônicos (International Organization for Standardization, 2013). O aumento das transações online e a necessidade de compliance com regulamentações de segurança têm impulsionado a adoção desses aplicativos, tornando-os uma parte crítica da infraestrutura digital moderna (European Union, 1999).

O AssinApp surgiu em resposta a essa necessidade, oferecendo uma solução adaptada às demandas específicas do mercado brasileiro, conforme estabelece (Brasil, 2003). Ao compreender o contexto em que esses aplicativos operam, pode-se identificar as principais expectativas dos usuários e os desafios que devem ser superados.

## 5.2 Sobre o Aplicativo AssinApp

O AssinApp é um aplicativo móvel projetado para facilitar a assinatura digital de documentos, oferecendo uma solução segura e eficiente para a gestão de assinaturas eletrônicas. Desenvolvido com o intuito atuar como alternativa a fim de que o usuário possa superar as limitações relativas a qualquer tipo de burocracia envolvida no processo de assinatura de documentos físicos.

O aplicativo faz uso da combinação de uma interface intuitiva com medidas de segurança em sua implementação, proporcionando assim funcionalidades determinantes para a assinatura e verificação de documentos.

Sua interface é projetada para ser amigável e de fácil navegação, simplificando o

processo de assinatura e verificação. Isso reduz a complexidade e o tempo necessário para completar essas tarefas, tornando o uso do aplicativo mais acessível para todos os tipos de usuários.

A segurança é uma prioridade no AssinApp, que utiliza algoritmos de criptografia para proteger documentos e assinaturas. Isso garante que as informações permaneçam seguras contra fraudes e acessos não autorizados. O aplicativo também oferece funcionalidades de registro e login, com autenticação reforçada para assegurar a identidade dos assinantes e administradores.

## 5.3 Personas

A partir das avaliações dos aplicativos de assinatura digital no Brasil, identificou-se a necessidade de criar personas detalhadas para guiar o desenvolvimento e a melhoria contínua desses aplicativos. As personas são representações fictícias, porém realistas, dos usuários finais de um produto. Elas são criadas com base em dados reais e visam ajudar a compreender as necessidades, comportamentos e objetivos dos usuários. Como descrito por Cooper et al., "Personas are archetypal users whose goals and characteristics represent the needs of a larger group of users, serving as a design target" (COOPER; REIMANN; CRONIN, 1999).

Para criar as personas, utilizou-se uma abordagem estruturada baseada na análise de avaliações e pesquisas de mercado sobre os aplicativos de assinatura digital presentes no Brasil. Os dados coletados foram analisados para identificar padrões de comportamento, necessidades e frustrações comuns entre os usuários. Com base nessa análise, os usuários foram segmentados em grupos distintos, cada um com características e objetivos específicos, resultando na criação de personas detalhadas que incluem informações demográficas, biografia, objetivos, frustrações e comportamentos de uso.

Em resumo, a criação dessas personas permite uma melhor compreensão dos diferentes perfis de usuários dos aplicativos de assinatura digital, orientando o desenvolvimento de funcionalidades e interfaces que atendam de forma mais eficaz às necessidades e expectativas desses usuários. A metodologia adotada garantiu a identificação precisa das necessidades e desafios dos usuários, resultando em personas que refletem fielmente os diversos segmentos de mercado para os quais o aplicativo é destinado.

A seguir, são apresentadas as personas detalhadas que representam os diferentes perfis de usuários do aplicativo de assinatura digital. Cada persona reflete padrões comportamentais e necessidades identificadas nas pesquisas realizadas. A persona primária representa um advogado corporativo que valoriza a segurança e a eficiência (Figura 8). Já a persona secundária reflete o perfil de uma freelancer de design que busca flexibilidade e praticidade (Figura 9). Por fim, a antipersona ilustra um usuário com baixa familiaridade

tecnológica, preferindo métodos tradicionais de assinatura (Figura 10).

### Persona primária - João

Figura 8 – Persona João


*Fonte: Autor*

#### Biografia

João é um advogado corporativo de 30 anos que trabalha em um grande escritório de advocacia em São Paulo. Ele valoriza a eficiência e a segurança em seu trabalho, frequentemente lidando com contratos importantes. João gosta de praticar esportes como tênis e corrida no parque nos finais de semana.

#### Dores

- Preocupações com a validade legal e segurança das assinaturas digitais.
- Ferramentas complicadas que exigem muitos passos para concluir a assinatura.
- Falta de integração com outros softwares jurídicos.
- Demora na aprovação e retorno dos documentos assinados.
- Alto custo de algumas soluções de assinatura digital.

#### Objetivos

- Assinar contratos de forma rápida e segura, sem necessidade de reuniões presenciais.
- Garantir a conformidade legal e a segurança das assinaturas.

- Automatizar processos repetitivos para ganhar mais tempo para tarefas estratégicas.
- Melhorar a produtividade da equipe jurídica.
- Reduzir a quantidade de papel utilizado no escritório.

### Histórias de usuário

João recebe contratos por e-mail, abre o aplicativo no laptop para revisar, assina digitalmente e envia de volta. Ele utiliza o aplicativo diariamente para revisar e assinar documentos importantes, garantindo que todas as assinaturas sejam válidas e seguras.

### Persona secundária - Ana

Figura 9 – Persona Ana


*Fonte: Autor*

### Biografia

Ana é uma freelancer de design de 25 anos que reside no Rio de Janeiro. Ela trabalha com clientes de diversas partes do mundo e valoriza a flexibilidade no trabalho. Ana gosta de viajar e praticar fotografia nos tempos livres.

### Dores

- Encontrar aplicativos complicados de usar e caros.
- Processos de assinatura que requerem muitas etapas.
- Dificuldade em acompanhar o status dos contratos assinados.

- Falta de suporte ao cliente em algumas plataformas.
- Limitações em dispositivos móveis que afetam a usabilidade.

### Objetivos

- Facilitar a assinatura de contratos com clientes internacionais.
- Melhorar a eficiência na gestão de documentos.
- Reduzir o tempo gasto com processos administrativos.
- Aumentar a satisfação dos clientes com processos rápidos e simples.
- Garantir que todos os contratos estejam devidamente assinados e arquivados.

### Histórias de usuário

Ana recebe um contrato de um cliente, abre o aplicativo no smartphone, revisa, assina digitalmente e envia de volta. Ela utiliza o aplicativo sempre que precisa fechar um novo contrato, em média semanalmente, buscando uma solução que torne a assinatura de contratos rápida e fácil, sem complicações.

### Antipersona - Paulo

Figura 10 – Antipersona Paulo


*Fonte: Autor*

### Biografia

Paulo é um pequeno empresário de 50 anos que gerencia uma empresa em Curitiba. Ele tem pouca familiaridade com tecnologia e prefere métodos tradicionais. Paulo gosta de jardinagem e atividades ao ar livre nos tempos livres.

### Dores

- Dificuldade em usar tecnologias digitais.
- Processos confusos e difíceis de entender.
- Preocupações com a segurança e a validade legal das assinaturas digitais.
- Falta de suporte técnico adequado.
- Preferência por métodos tradicionais, como papel e caneta.

### Objetivos

- Assinar documentos necessários para o negócio sem complicações.
- Manter os processos simples e compreensíveis.
- Garantir a segurança e a validade legal dos documentos assinados.
- Receber suporte técnico confiável para resolver problemas.

### Histórias de usuário

Paulo recebe um documento importante por e-mail, mas prefere imprimi-lo, assiná-lo manualmente e escaneá-lo de volta. Ele usa métodos tradicionais sempre que possível, sentindo-se frustrado com a dificuldade em usar tecnologias digitais para assinatura de documentos.

## 5.4 Estudo de soluções similares

A realização de um estudo de aplicativos similares desempenha um papel vital no desenvolvimento de nosso aplicativo de assinatura digital. Ao analisar as funcionalidades, a usabilidade e as soluções tecnológicas presentes em outras plataformas, especialmente em aplicativos consolidados como o *GOV.BR*, foi possível identificar padrões de mercado,

melhores práticas e potenciais áreas de inovação. Esse processo proporcionou entendimento a respeito do que já foi eficaz, o que pode ser aprimorado e como diferenciar a solução proposta das demais existentes no mercado.

Nesta seção, apresentamos uma análise de aplicativos que oferecem funcionalidades similares ao aplicativo de assinatura digital proposto. Esta análise inclui uma descrição das principais funcionalidades, bem como uma avaliação dos pontos fortes e fracos de cada aplicativo.

Foi necessário realizar uma pesquisa detalhada sobre outros aplicativos disponíveis no mercado. O objetivo desta pesquisa foi identificar as funcionalidades oferecidas, bem como os pontos positivos e negativos de cada um, a fim de obter uma visão abrangente do panorama atual.

Para isso, foi utilizada uma abordagem prática e teórica. Primeiramente, foi instalado e testado diversos aplicativos de assinatura digital na Play Store. Durante o teste, foi explorado as principais funcionalidades oferecidas por cada aplicativo, como a facilidade de uso, a velocidade de processamento de assinaturas, a presença ou ausência de anúncios, a gratuidade das funcionalidades, e a capacidade de integração e exportação de documentos.

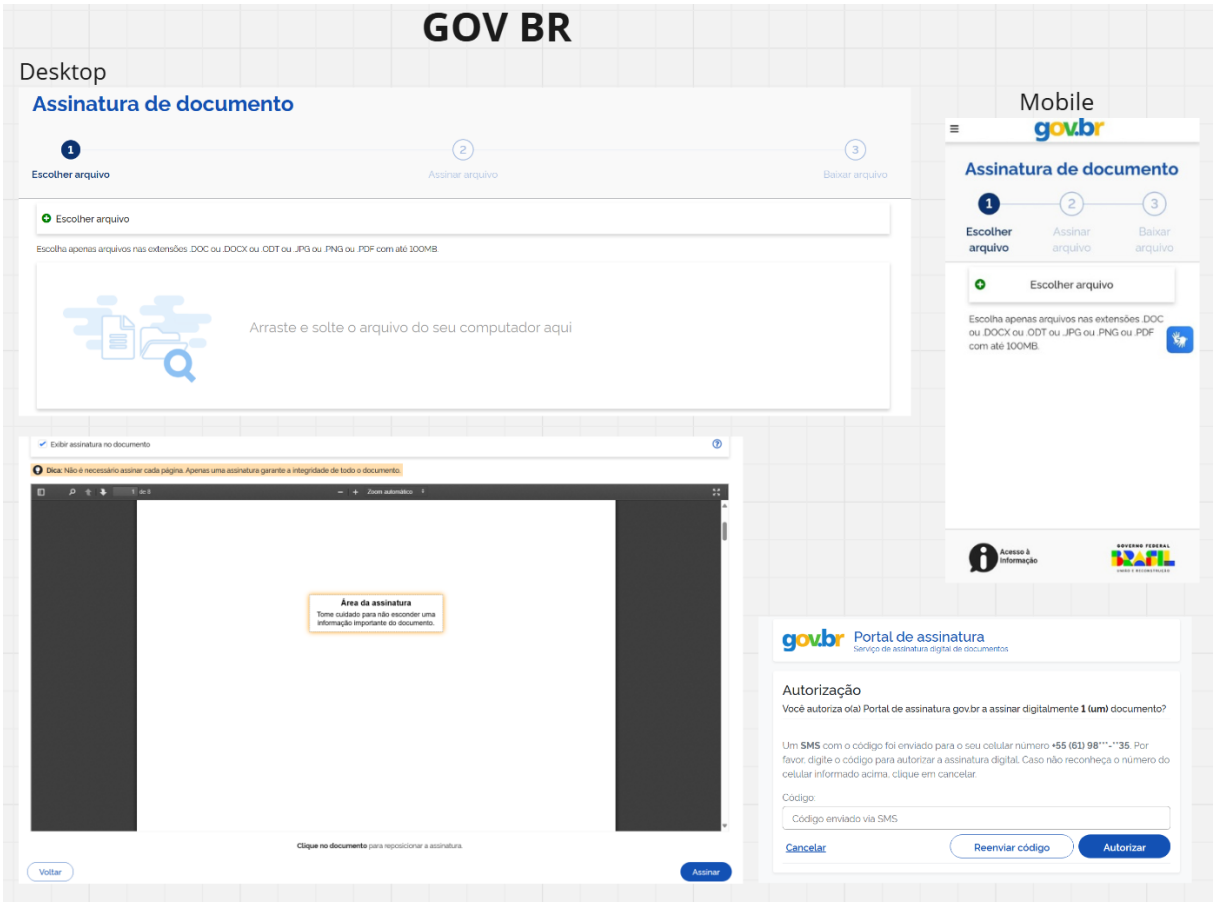
Além da experiência prática com os aplicativos, foi realizada uma análise minuciosa das avaliações de usuários na Play Store. As avaliações fornecidas pelos usuários são uma fonte valiosa de feedback, pois refletem experiências reais e variadas com o aplicativo. Essas avaliações foram examinadas para identificar padrões nos comentários, tanto positivos quanto negativos.

### 5.4.1 GOV.BR

O GOV.BR Assinatura Digital é uma plataforma desenvolvida pelo governo brasileiro que permite a assinatura digital de documentos oficiais e governamentais. A ferramenta utiliza certificados digitais para autenticação, garantindo a segurança e a integridade dos documentos assinados. Ela está integrada aos serviços públicos digitais, facilitando o acesso e a gestão de documentos oficiais pelos cidadãos e pelas instituições públicas (GOV.BR, 2022).

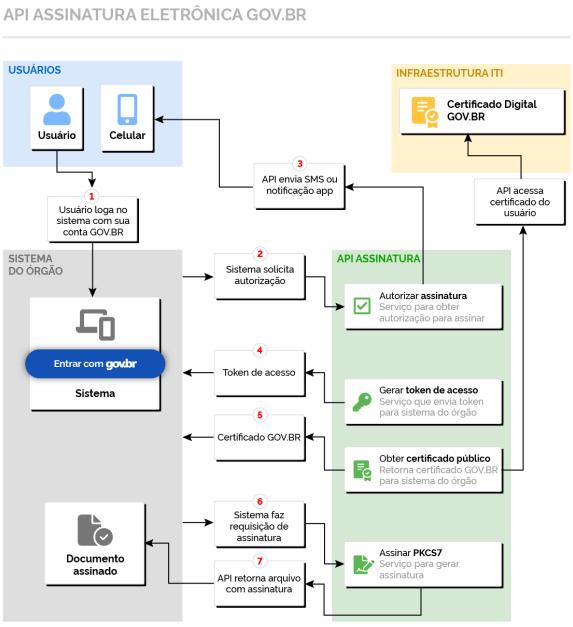
A Figura 11 apresenta a interface do GOV.BR, destacando suas principais funcionalidades e a integração com outros serviços públicos digitais. Já a Figura 12 ilustra o fluxo da API de assinatura do GOV.BR, destacando como ocorrem os processos de autenticação e assinatura.

Figura 11 – GOV.BR




*Fonte: Autor*

Figura 12 – Fluxo API GOV.BR




*Fonte: GOV.BR*

#### Funcionalidades

- Assinatura digital de documentos governamentais
- Suporte para autenticação via certificados digitais
- Integrado aos serviços públicos digitais

#### Pontos Positivos

- Elevado nível de segurança e conformidade com regulamentações
- Facilita a autenticação em serviços públicos

#### Pontos Negativos

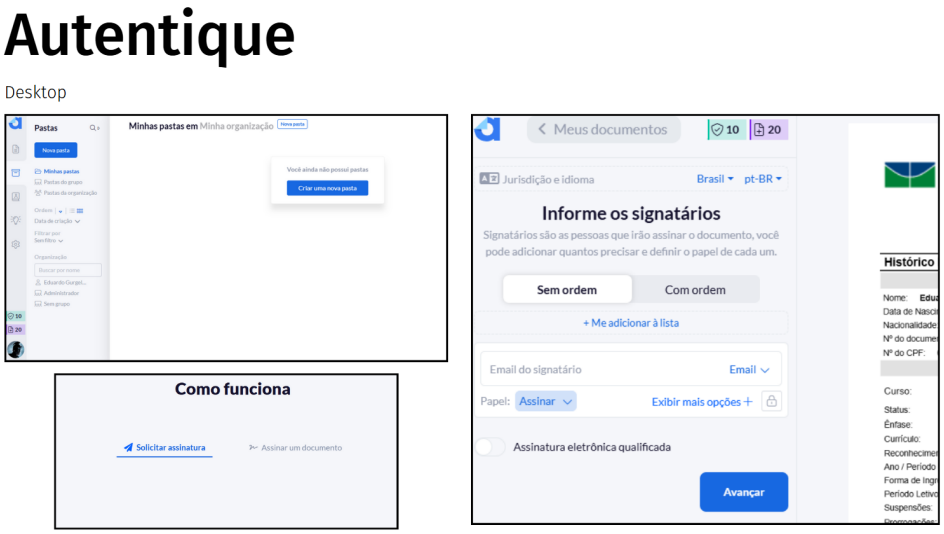
- Funcionalidades limitadas comparadas a aplicativos comerciais
- Interface menos amigável

### 5.4.2 Autentique

O Autentique é uma plataforma digital especializada em facilitar e agilizar o processo de assinatura eletrônica de documentos, permitindo que usuários enviem, assinem e validem documentos de maneira segura e legalmente reconhecida. A plataforma oferece suporte a múltiplos tipos de assinatura, incluindo assinaturas eletrônicas avançadas e qualificadas, com ou sem o uso de certificados digitais, adaptando-se às necessidades específicas de cada documento e garantindo conformidade com as normas legais vigentes.

A Figura 13 apresenta a interface do Autentique, destacando suas funcionalidades principais.

Figura 13 – Autentique




*Fonte: Autor*

### Funcionalidades

O Autentique é uma plataforma projetada para facilitar a assinatura digital de documentos. O processo começa com a seleção do arquivo ou modelo que se deseja assinar, seguido da indicação dos signatários e das respectivas formas de validação. O usuário pode então posicionar as assinaturas no local desejado dentro do documento. Após esses passos, o documento é enviado para assinatura, e o usuário será notificado assim que todos os signatários completarem o processo.

### Pontos Positivos

- **Variedade de Tipos de Assinatura**: O Autentique suporta tanto assinaturas eletrônicas avançadas quanto qualificadas, oferecendo flexibilidade ao usuário na escolha do método de assinatura mais adequado ao seu documento. A plataforma é compatível com assinaturas que não exigem certificado digital, utilizando verificações por email, SMS, WhatsApp, validação de CPF, validação documental, ou biometria facial.
- **Compatibilidade com Certificados Digitais**: Para documentos que exigem maior rigor, a plataforma permite o uso de certificados digitais, como o Certificado A1 (Arquivo) e Certificado A3 (Token USB ou Smartcard), alinhando-se às normas da ICP-Brasil.
- **Planos Flexíveis**: O Autentique oferece um plano gratuito com até 20 documentos por mês e usuários ilimitados, além de um plano corporativo que permite o envio de documentos ilimitados, personalização de emails, lembretes de assinatura e lembretes de vencimento, atendendo tanto usuários individuais quanto corporativos.

- **Facilidade de Uso**: O processo de assinatura é intuitivo e guiado, desde a seleção do documento até o envio para os signatários, tornando a experiência fluida e acessível para todos os níveis de usuário.

### Pontos Negativos

- **Limitações no Plano Gratuito**: Embora o plano gratuito seja útil para usuários ocasionais, o limite de 20 documentos por mês pode ser insuficiente para aqueles que precisam assinar ou gerenciar um volume maior de documentos. Além disso, algumas funcionalidades, como a personalização de emails e lembretes de vencimento, estão disponíveis apenas nos planos pagos.
- **Necessidade de Certificado Digital para Assinaturas Qualificadas**: Para utilizar a assinatura eletrônica qualificada, é necessário adquirir e gerenciar um certificado digital, o que pode ser um obstáculo para usuários que não estão familiarizados com esses requisitos ou que preferem evitar custos adicionais.
- **Custo para Planos Corporativos**: Embora o plano corporativo ofereça funcionalidades avançadas, o custo de 99 reais por mês pode ser considerado alto para pequenas empresas ou freelancers que estão começando e não têm necessidade de enviar um grande número de documentos.

### Quadro Resumo:

O Quadro Resumo 4 apresenta uma análise dos recursos do Autentique, destacando tanto os pontos positivos quanto os negativos da plataforma, o que facilita a compreensão das suas funcionalidades e limitações.

Tabela 4 – Análise dos Recursos do Autentique

| **Categoria** | **Pontos Positivos** | **Pontos Negativos** |
|---|---|---|
| Variedade de Tipos de Assinatura | Suporte a assinaturas eletrônicas avançadas e qualificadas | Necessidade de certificado digital para assinaturas qualificadas |
| Compatibilidade com Certificados Digitais | Alinhamento às normas da ICP-Brasil | Gerenciamento de certificados pode ser complexo para alguns usuários |
| Planos Flexíveis | Opções gratuitas e corporativas com diferentes níveis de funcionalidade | Limitações no plano gratuito e custo do plano corporativo |
| Facilidade de Uso | Processo intuitivo e guiado | - |

### 5.4.3 Assine PDF

O Assine PDF é um aplicativo móvel projetado para permitir que os usuários assinem documentos PDF de maneira prática e segura diretamente em seus dispositivos. Focado em simplicidade e acessibilidade, o aplicativo se destaca por permitir assinaturas desenhadas à mão, utilizando o dedo ou uma caneta touch, oferecendo uma solução rápida e eficiente para a assinatura digital de documentos em diversos contextos, desde o pessoal até o profissional.

A Figura 14 apresenta a interface do Assine PDF, destacando suas principais funcionalidades para a assinatura digital de documentos PDF.

Figura 14 – Assine PDF


*Fonte: Autor*

#### 5.4.3.1 Funcionalidades

O Assine PDF é principalmente utilizado para assinar documentos PDF diretamente no telefone. A funcionalidade principal do aplicativo é permitir que os usuários assinem documentos escrevendo no telefone, seja com o dedo ou com uma caneta touch. Além disso, o aplicativo oferece uma série de melhorias recentes, como a possibilidade de assinar em várias cores (azul, preto, cinza, verde), proteção dos arquivos assinados com senha, um novo design moderno baseado no Material Design 3, um processo simplificado para salvar e compartilhar documentos, além de funcionalidades avançadas como botões de desfazer e refazer ações e a integração com uma Plataforma de Gestão de Consentimento certificada pelo Google.

### Pontos Positivos

Facilidade de Uso: Muitos usuários elogiam a simplicidade e praticidade do aplicativo. Comentários como "Prático e fácil de usar," "Super simples e fácil," e "Fácil de utilizar e funcional" são frequentes. Isso mostra que o aplicativo atende bem às necessidades de quem precisa assinar documentos rapidamente sem complicações.

Gratuito: A ausência de custos é um ponto muito apreciado, com usuários destacando que, apesar das propagandas, o fato de ser gratuito é um grande atrativo.

Qualidade da Assinatura: Vários usuários mencionaram que a qualidade da assinatura é boa, mesmo quando feita com o dedo. Comentários como "A assinatura fica com ótima qualidade" e "Minha assinatura saiu praticamente igual ao do papel" demonstram isso.

Rapidez: O aplicativo é elogiado por sua rapidez, com muitos comentários mencionando que é possível assinar documentos em poucos minutos, como "Muito rápido e prático" e "Rápido e direto."

### Pontos Negativos

Propagandas Excessivas: Um dos principais pontos negativos mencionados é a quantidade de anúncios. Comentários como "Muita propaganda isso é muito irritante" e "Horrível fica travado em propaganda" são recorrentes, indicando que isso é um problema significativo para os usuários.

Problemas de Usabilidade: Alguns usuários relataram dificuldades específicas, como problemas para encontrar e carregar arquivos, a necessidade de reabrir o documento para múltiplas assinaturas, e a falta de recursos como desfazer a última ação ou salvar assinaturas para reutilização. Comentários incluem "O aplicativo não consegue encontrar nem arquivos no drive nem no dispositivo" e "Não permite salvar uma assinatura para reutilizar."

Falta de Funcionalidades: Há várias sugestões para melhorias, como adicionar a opção de assinar em diferentes cores (especialmente azul), girar a tela para assinaturas mais longas, e copiar e colar assinaturas. Comentários como "Poderia ter cores e abrir a tela de assinatura também na horizontal" e "Faltou permitir mudar a cor da caneta para azul" são exemplos disso.

Problemas Técnicos: Alguns usuários relataram falhas técnicas, como o aplicativo travando, não salvando assinaturas corretamente, ou distorcendo as assinaturas. Comentários incluem "App só fica carregando e não consigo usá-lo" e "A letra sai torta e se errou tem só uma chance de fazer."

#### Quadro Resumo:

O Quadro Resumo 5 apresenta uma análise dos comentários sobre o Assine PDF, destacando tanto os pontos positivos quanto os negativos apontados pelos usuários, fornecendo uma visão abrangente sobre a experiência com o aplicativo.

Tabela 5 – Análise dos Comentários do AssinePDF

| Categoria | Pontos Positivos | Pontos Negativos |
|---|---|---|
| Facilidade de Uso | Simples e prático, fácil de usar, intuitivo | Propagandas excessivas, problemas de usabilidade |
| Gratuito | Sem custo para os usuários | Propagandas irritantes |
| Qualidade da Assinatura | Alta qualidade, semelhante à assinatura no papel | Dificuldades técnicas e distorção da assinatura |
| Funcionalidades | Rapidez na assinatura, interface direta | Falta de funcionalidades (cores, copiar/colar, girar tela) |
| Problemas Técnicos | - | Travamentos, dificuldade para encontrar arquivos, necessidade de reabrir documentos |

### 5.4.4 DocuSign

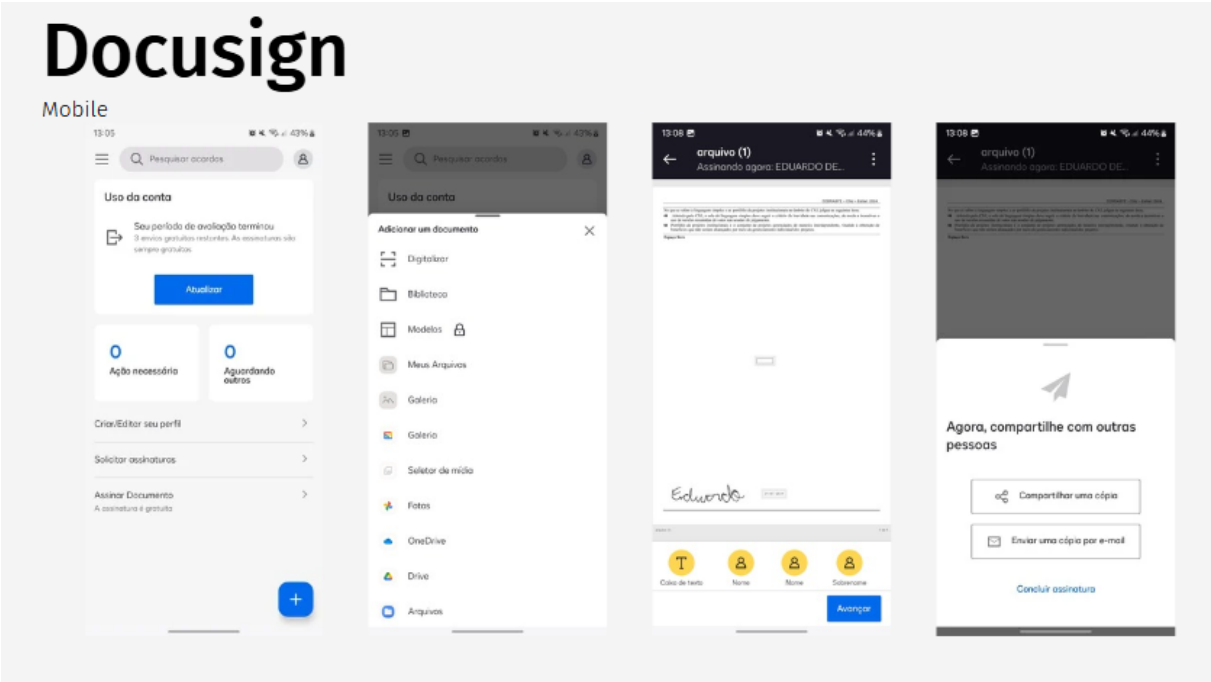
#### Contexto

O DocuSign é uma solução líder em gestão de acordos eletrônicos que facilita a criação, verificação, negociação, assinatura e administração de contratos de forma totalmente digital. A plataforma é projetada para oferecer uma experiência de assinatura intuitiva e segura, permitindo que usuários em qualquer dispositivo assinem documentos de forma rápida e conforme as regulamentações legais. Além disso, o DocuSign se integra facilmente com sistemas corporativos e automatiza fluxos de trabalho, otimizando o processo de gestão de contratos para empresas de todos os tamanhos. Sua interface, bem como funcionalidades principais, podem ser vistas na Figura 15.

#### Funcionalidades

O DocuSign é uma ferramenta robusta e amplamente utilizada para a assinatura digital de documentos. Ele oferece uma interface intuitiva que permite aos usuários assinar, enviar e gerenciar documentos de forma eletrônica, garantindo validade jurídica e economizando tempo.

Figura 15 – DocuSign




*Fonte: Autor*

### Pontos Positivos

Facilidade de Uso: Muitos usuários elogiam a interface intuitiva e a facilidade de uso do aplicativo. Comentários como “Simples e prático” e “Muito fácil de usar” são comuns, destacando que o aplicativo facilita o processo de assinatura digital.

Rapidez e Eficiência: A rapidez com que os documentos podem ser assinados e processados é um ponto forte, com usuários destacando a agilidade do aplicativo. Exemplos incluem “Rápido e eficiente” e “Assinatura rápida e legível.”

Funcionalidades Úteis: O DocuSign oferece uma série de funcionalidades que são vistas como úteis pelos usuários, como a capacidade de enviar documentos diretamente pelo app e integrar com serviços de armazenamento. Comentários como “Facilita demais os processos de contrato e assinaturas” são indicativos disso.

Confiabilidade e Segurança: A confiabilidade e segurança do DocuSign são frequentemente mencionadas, com usuários confiando na validade jurídica das assinaturas feitas pelo aplicativo. Comentários como “Funciona super bem” e “Validade jurídica” reforçam esse ponto.

### Pontos Negativos

Problemas Técnicos: Alguns usuários relatam problemas técnicos, como travamentos e dificuldades para carregar documentos. Comentários como “Deu muito erro para

abrir os arquivos" e "Fica carregando durante um longo tempo e dá erro" ilustram essas dificuldades.

Propagandas e Planos Pagos: Há queixas sobre o custo dos planos pagos, especialmente para usuários brasileiros, que consideram os valores elevados. Comentários como "Ter que pagar um absurdo em dólar" e "Preço exorbitante" são comuns.

Usabilidade: Alguns usuários mencionam que a interface pode ser confusa ou contra-intuitiva em certos aspectos. Comentários como "Muito contra intuitivo" e "Informações não são claras e objetivas" indicam que há espaço para melhorias na experiência do usuário.

Problemas com Cobrança e Cancelamento: Vários usuários enfrentaram problemas ao tentar cancelar suas assinaturas ou com cobranças inesperadas. Comentários como "Não consigo cancelar minha conta" e "Problemas na cobrança" refletem essas dificuldades.

### Quadro Resumo

A Tabela 6 apresenta uma análise detalhada dos comentários dos usuários sobre o DocuSign. Ela está dividida em categorias que destacam os pontos positivos e negativos, proporcionando uma visão geral das principais características e desafios encontrados pelos usuários ao utilizar o aplicativo.

Tabela 6 – Análise dos Comentários do DocuSign

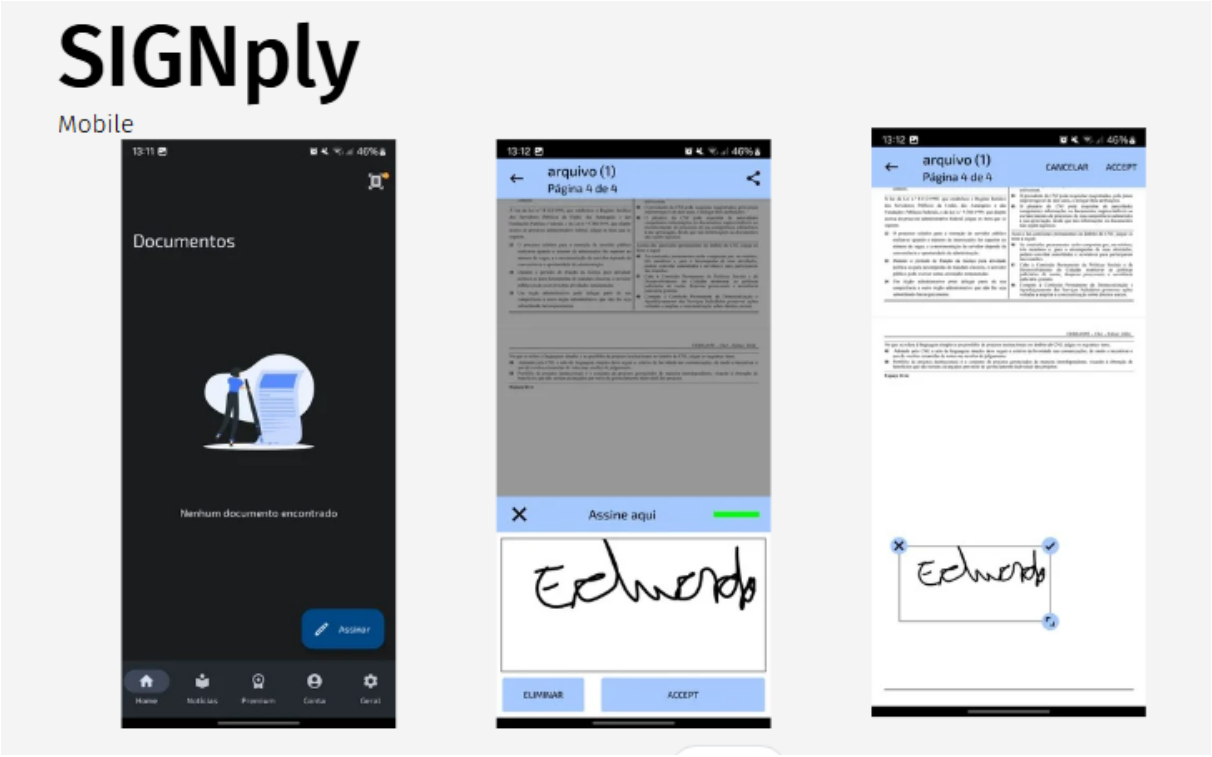
| **Categoria** | **Pontos Positivos** | **Pontos Negativos** |
|---|---|---|
| Facilidade de Uso | Interface intuitiva, fácil de usar | Interface contra-intuitiva em alguns aspectos |
| Rapidez e Eficiência | Assinatura rápida, processa documentos rapidamente | Travamentos e lentidão ao carregar documentos |
| Funcionalidades Úteis | Envio direto de documentos, integração com serviços de armazenamento | - |
| Confiabilidade e Segurança | Validade jurídica, confiável | - |
| Propagandas e Planos Pagos | - | Custo elevado dos planos pagos |
| Problemas com Cobrança e Cancelamento | - | Dificuldades para cancelar assinatura, cobranças inesperadas |

### 5.4.5 SIGNply

#### Contexto

Como ilustrado na Figura 16, SIGNply é uma solução de assinatura digital projetada especificamente para dispositivos móveis, oferecendo uma maneira simples e legalmente válida de assinar documentos e formulários digitais. A plataforma está alinhada com a normativa europeia eIDAS, o que garante que as assinaturas realizadas através do SIGNply sejam consideradas assinaturas avançadas. Com versões que vão desde uma gratuita para uso profissional com baixo volume de documentos até uma versão premium com funcionalidades avançadas, o SIGNply é adaptável tanto para freelancers quanto para grandes corporações.

Figura 16 – SIGNply




*Fonte: Autor*

#### Funcionalidades

O Signply é um aplicativo projetado para facilitar a assinatura digital de documentos PDF diretamente em dispositivos móveis. Ele se destaca por sua simplicidade e pela ausência de anúncios, o que o torna uma ferramenta prática para usuários que precisam assinar documentos rapidamente e sem complicações.

### Pontos Positivos

Facilidade de Uso: Muitos usuários destacam a facilidade de uso do aplicativo, mencionando que ele é intuitivo e direto ao ponto. Comentários como “Prático, intuitivo e fácil de usar” e “Simples e objetivo” são comuns, destacando a usabilidade do app.

Rapidez e Eficiência: O Signply é elogiado pela rapidez com que permite assinar documentos. Comentários como “Muito rápido e prático” e “Cumpre o que promete” mostram que os usuários valorizam a eficiência do aplicativo.

Ausência de Anúncios: A ausência de anúncios é frequentemente mencionada como um ponto positivo, proporcionando uma experiência de usuário mais limpa e sem interrupções. Exemplos incluem “Sem anúncios e sem dificuldades” e “Muito bom, sem propagandas.”

Funcionalidades Gratuitas: A gratuidade do aplicativo é vista como um grande atrativo, especialmente quando comparado a outros aplicativos que cobram por funcionalidades similares. Comentários como “100% gratuito” e “Sem custos” reforçam isso.

### Pontos Negativos

Problemas Técnicos: Muitos usuários relatam problemas técnicos recorrentes, como falhas na atualização, erros de licença expirada, e dificuldades para salvar ou compartilhar assinaturas. Comentários como “Licença expirada” e “Não consigo atualizar” são exemplos dessas frustrações.

Usabilidade: Apesar de ser fácil de usar, alguns usuários sugerem melhorias na usabilidade, como a adição de uma função de desfazer, a capacidade de salvar assinaturas para reutilização, e melhor sensibilidade ao toque. Comentários como “Falta a função desfazer” e “Não salva a assinatura” refletem essas necessidades.

Integração e Exportação: Há queixas sobre dificuldades para integrar com outras ferramentas ou exportar documentos assinados de forma eficaz. Comentários como “Assinatura não aparece ao compartilhar” e “Dificuldade para salvar documentos” indicam esses problemas.

Problemas com Sensibilidade: Alguns usuários relatam que a área de assinatura é muito sensível, o que torna difícil obter uma assinatura precisa. Comentários como “Muito sensível ao toque” destacam essa questão.

### Quadro Resumo

Os comentários dos usuários sobre o SIGNply estão resumidos na Tabela 7, que fornece uma visão geral das funcionalidades e dificuldades relatadas.

Tabela 7 – Análise dos Comentários do Signply

| **Categoria** | **Pontos Positivos** | **Pontos Negativos** |
|---|---|---|
| Facilidade de Uso | Intuitivo, fácil de usar | Necessidade de função de desfazer, melhor sensibilidade ao toque |
| Rapidez e Eficiência | Assinatura rápida, processa documentos rapidamente | Erros técnicos recorrentes, problemas de licença expirada |
| Ausência de Anúncios | Experiência limpa e sem interrupções | - |
| Funcionalidades Gratuitas | 100% gratuito, sem custos | Dificuldades para salvar e compartilhar assinaturas |
| Integração e Exportação | - | Problemas para integrar com outras ferramentas, dificuldade para exportar documentos |

### 5.4.6 Critérios de Comparação

Para analisar as soluções disponíveis no mercado e comparar com o AssinApp, foram definidos os seguintes critérios:

- **Custo:** Se a solução é gratuita ou possui algum custo para os usuários.
- **Usabilidade:** Facilidade de uso e acessibilidade da interface.
- **Integração:** Capacidade de integração com outras plataformas e serviços.
- **Privacidade e Segurança:** Proteção dos dados do usuário e conformidade com normas regulatórias.
- **Acessibilidade:** Recursos que tornam a solução utilizável para diferentes perfis de usuários.

#### 5.4.6.1 Tabela Comparativa

A Tabela 8 apresenta um comparativo entre diferentes soluções disponíveis no mercado e o AssinApp.

Tabela 8 – Comparação entre soluções de assinatura digital

| **Critério** | **GOV.BR Assinaturas** | **Autentique** | **AssinePDF** | **DocuSign** | **Signply** | **AssinApp** |
|---|---|---|---|---|---|---|
| **Custo** | Gratuito | Freemium | Gratuito | Pago | Freemium | Gratuito |
| **Usabilidade** | Média | Alta | Baixa | Alta | Média | Alta |

| Critério | GOV.BR Assinaturas | Autentique | AssinePDF | DocuSign | Signply | AssinApp |
|---|---|---|---|---|---|---|
| **Integração** | Sim | Sim | Não | Sim | Sim | Sim |
| **Privacidade e Segurança** | Alta | Média | Baixa | Alta | Média | Alta |
| **Acessibilidade** | Média | Média | Baixa | Alta | Média | Alta |

#### 5.4.6.2 Diferenciais do AssinApp

Com base na análise comparativa, o AssinApp apresenta os seguintes diferenciais:

- **Gratuidade completa**, sem necessidade de planos pagos ou restrições de funcionalidades essenciais.
- **Interface intuitiva**, permitindo que usuários com diferentes níveis de familiaridade com tecnologia realizem assinaturas digitais sem dificuldades.
- **Maior acessibilidade**, considerando boas práticas para usuários com deficiência ou baixa familiaridade tecnológica.
- **Privacidade reforçada**, garantindo que os dados do usuário sejam processados localmente sem dependência de armazenamento em nuvem de terceiros.

#### 5.4.6.3 Conclusão da Comparação

A partir da análise realizada, observa-se que o AssinApp preenche lacunas deixadas por outras soluções disponíveis no mercado. Enquanto plataformas como GOV.BR Assinaturas garantem segurança, sua usabilidade é mais limitada. Outras soluções, como Autentique e Signply, apresentam maior facilidade de uso, mas carecem de suporte mais amplo a integrações.

Dessa forma, o AssinApp se posiciona como uma alternativa viável e acessível, oferecendo um conjunto equilibrado de funcionalidades, sem custos adicionais para os usuários e com um forte compromisso com a segurança e a privacidade. Isso reforça sua relevância dentro do contexto da pesquisa-ação realizada no presente trabalho.

## 5.5 Requisitos

### 5.5.1 Explicação dos Requisitos

Os requisitos do sistema são essenciais para definir as funcionalidades e características que o aplicativo de assinatura digital deve atender. Eles são divididos em dois tipos principais: **Requisitos Funcionais** e **Requisitos Não Funcionais**.

- **Requisitos Funcionais (RF)**: Descrevem as funcionalidades específicas que o sistema deve possuir. Por exemplo, a capacidade de permitir que os usuários assinem documentos digitalmente, armazenem e compartilhem esses documentos (MAXIM, 2020).
- **Requisitos Não Funcionais (RNF)**: Descrevem as características gerais do sistema, como desempenho, segurança e usabilidade (BASS PAUL CLEMENTS, 2003). Esses requisitos garantem que o sistema funcione corretamente sob certas condições e mantenha um bom nível de qualidade ISO/IEC (2011).

A Tabela 9 apresenta os principais requisitos do sistema, juntamente com um código único que será utilizado para referência ao longo do desenvolvimento.

### 5.5.2 Tabela de Requisitos

Entre os requisitos funcionais, o sistema deve permitir que os usuários criem contas (RF01) e façam login (RF02) com e-mail e senha. Também deve permitir o upload de documentos (RF03), assinatura digital desses documentos (RF04) e o compartilhamento de documentos assinados via e-mail (RF05).

Nos requisitos não funcionais, o sistema deve garantir a segurança das comunicações com criptografia SSL/TLS (RNF01) e suportar até 1000 usuários simultâneos sem perder desempenho (RNF02). O tempo de resposta para assinatura deve ser inferior a 2 segundos (RNF03), e o sistema deve ser compatível com dispositivos móveis Android (RNF04). Além disso, todos os dados devem ser armazenados com segurança e backup automático (RNF05).

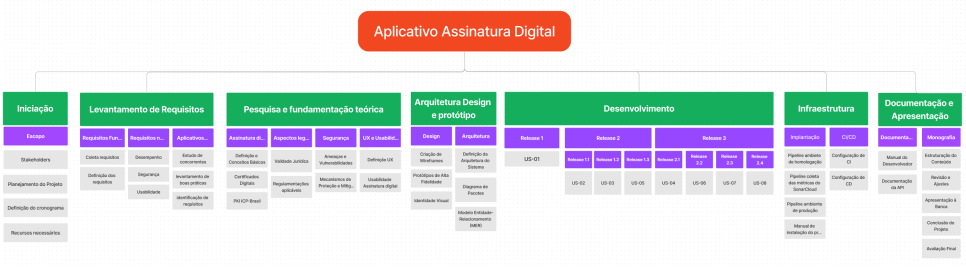
A tabela antes apresentada organiza de maneira clara e objetiva os requisitos funcionais e não funcionais que o sistema de assinatura digital deve atender. Os requisitos funcionais especificam as principais funcionalidades que o sistema deve oferecer aos usuários, como criação de conta, login, upload de documentos, assinatura digital e compartilhamento de documentos.

Tabela 9 – Requisitos do Sistema

| Código | Requisito |
|---|---|
| RF01 | O sistema deve permitir que o usuário crie uma conta utilizando e-mail e senha. |
| RF02 | O sistema deve permitir que o usuário faça login utilizando suas credenciais. |
| RF03 | O sistema deve permitir que o usuário faça upload de documentos para assinatura. |
| RF04 | O sistema deve permitir que o usuário assine digitalmente um documento. |
| RF05 | O sistema deve permitir que o usuário compartilhe documentos assinados via e-mail. |
| RNF01 | O sistema deve garantir que todas as comunicações sejam seguras usando criptografia SSL/TLS. |
| RNF02 | O sistema deve ser escalável para suportar o crescimento no número de usuários, garantindo uma experiência consistente sem degradação de desempenho. |
| RNF03 | O sistema deve ser capaz de realizar a autenticação multifator para todas as operações de assinatura. |
| RNF04 | O sistema deve ser compatível com dispositivos móveis (Android). |
| RNF05 | O sistema deve garantir que todos os dados sejam armazenados de forma segura, com backup automático. |

### 5.5.3 Estrutura Analítica do Projeto - EAP

Figura 17 – EAP




*Fonte: Autor*

Como mostrado na Figura 17, a Estrutura Analítica do Projeto (EAP) para o desenvolvimento do *Aplicativo de Assinatura Digital* foi elaborada para organizar de maneira estruturada todas as atividades necessárias para a conclusão do projeto, desde a fase de iniciação até a documentação e apresentação final (KERZNER, 2022). A EAP foi dividida em sete grandes áreas, cada uma representando uma fase essencial do projeto.

A fase de **Iniciação** abrangeu a definição do escopo, a identificação dos stakeholders, o planejamento geral do TCC, a definição do cronograma e a alocação dos recursos necessários. Em seguida, a fase de **Levantamento de Requisitos** envolveu a coleta e análise dos requisitos funcionais e não funcionais do aplicativo, além da análise comparativa com aplicativos similares.

A fase de **Pesquisa e Fundamentação Teórica** abordou estudos sobre conceitos de assinatura digital, aspectos legais, segurança, usabilidade e acessibilidade, que foram cruciais para embasar o desenvolvimento do aplicativo. Posteriormente, a fase de **Arquitetura, Design e Protótipo** focou na criação do design da interface, na definição da arquitetura do sistema e no desenvolvimento de protótipos de alta fidelidade.

O **Desenvolvimento** do aplicativo foi dividido em três *releases* principais, cada uma contendo incrementos nas funcionalidades. A fase de **Infraestrutura** foi dedicada à preparação e configuração do ambiente de desenvolvimento e produção, incluindo processos de Integração Contínua (CI) e Entrega Contínua (CD).

Por fim, a fase de **Documentação e Apresentação** compreendeu a criação de toda a documentação técnica e a preparação para a apresentação do TCC, culminando na **Conclusão do Projeto**, que envolveu a revisão final, a avaliação das lições aprendidas e a entrega definitiva do aplicativo e da monografia.

## 5.6 Identidade Visual

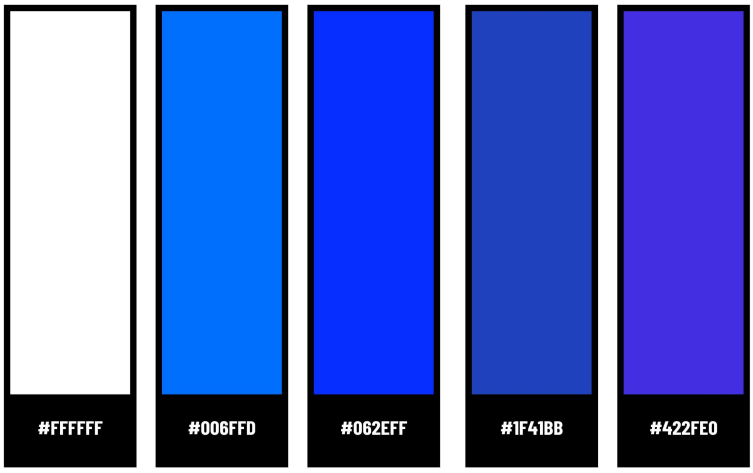
A Identidade Visual é composta por um conjunto de elementos gráficos e visuais que definem a interface do aplicativo. Estes elementos incluem a paleta de cores, logotipo, tipografia e o protótipo de alta fidelidade, todos projetados para garantir uma experiência intuitiva e acessível para o usuário.

### 5.6.1 Paleta de Cores

A paleta de cores do aplicativo, ilustrada na Figura 18, é composta por um conjunto harmônico de cores que garantem contraste adequado e uma identidade visual moderna. As cores predominantes são o roxo e o branco, proporcionando um equilíbrio entre sofisticação e acessibilidade. O contraste entre as cores foi testado utilizando a ferramenta de análise de contraste da Adobe[1], garantindo conformidade com as Diretrizes de Acessibilidade para o Conteúdo da Web (WCAG), que são pormenorizadamente exploradas em Nogueira et al. (2017).

[1] Disponível em: <https://color.adobe.com/pt/create/color-contrast-analyzer>. Acesso em: 28 jan. 2025.

Figura 18 – Paleta de Cores Utilizada no Projeto




*Fonte: Autor*

### 5.6.2 Logotipo

O logotipo do aplicativo foi projetado para representar visualmente a essência do AssinApp, destacando a prática da assinatura digital de forma clara e intuitiva. Seu design incorpora elementos gráficos que remetem ao ato de assinar documentos, reforçando a proposta central do sistema. Além disso, a identidade visual foi desenvolvida seguindo princípios de simplicidade e escalabilidade, garantindo boa legibilidade em diferentes tamanhos e dispositivos.

Para atender a diferentes cenários de uso dentro do aplicativo, foram criadas três variações do logotipo:

- **Logotipo principal**: Utilizado em telas e fundos com contraste adequado.
- **Logotipo alternativo**: Variante que se adapta a diferentes aplicações dentro do sistema.
- **Logotipo para fundo claro**: Desenvolvido especificamente para ser utilizado quando o fundo do aplicativo for branco, garantindo a visibilidade ideal.

As Figuras 19, 20 e 21 apresentam as três versões do logotipo.

Figura 19 – Logotipo Principal do Aplicativo AssinApp


*Fonte: Autor*

Figura 20 – Logotipo Alternativo do Aplicativo AssinApp


*Fonte: Autor*

Figura 21 – Logotipo para Fundo Claro do Aplicativo AssinApp


*Fonte: Autor*

### 5.6.3 Favicon

O favicon do aplicativo AssinApp, apresentado na Figura 22, foi desenvolvido para representar visualmente a identidade do sistema de maneira simples e eficaz. Ele consiste em dois lápis que, quando posicionados juntos, formam a letra "A". Esse design remete tanto ao conceito de assinatura, que é a principal funcionalidade do aplicativo, quanto à inicial do seu nome, reforçando sua identidade visual de forma intuitiva.

Figura 22 – Favicon do Aplicativo AssinApp

*Fonte: Autor*

### 5.6.4 Tipografia

A identidade tipográfica do aplicativo AssinApp foi definida com base em duas fontes complementares, visando proporcionar fluidez na experiência do usuário.

A **Fredoka**[2] foi escolhida como a fonte principal do aplicativo. Seu design arredondado e levemente compacto transmite um tom amigável e acessível, alinhando-se à proposta intuitiva do AssinApp. As letras robustas e bem espaçadas garantem uma leitura clara, especialmente em títulos e botões de ação, onde a ênfase visual é essencial.

Para complementar, a **Poppins**[3] foi definida como a fonte secundária, aplicada em textos corridos e descrições. Seu traço geométrico e versátil proporciona uma aparência moderna e profissional, garantindo excelente legibilidade em diferentes tamanhos. A Poppins é amplamente utilizada em interfaces digitais devido à sua clareza, tornando-a ideal para instruções e conteúdos informativos dentro do aplicativo.

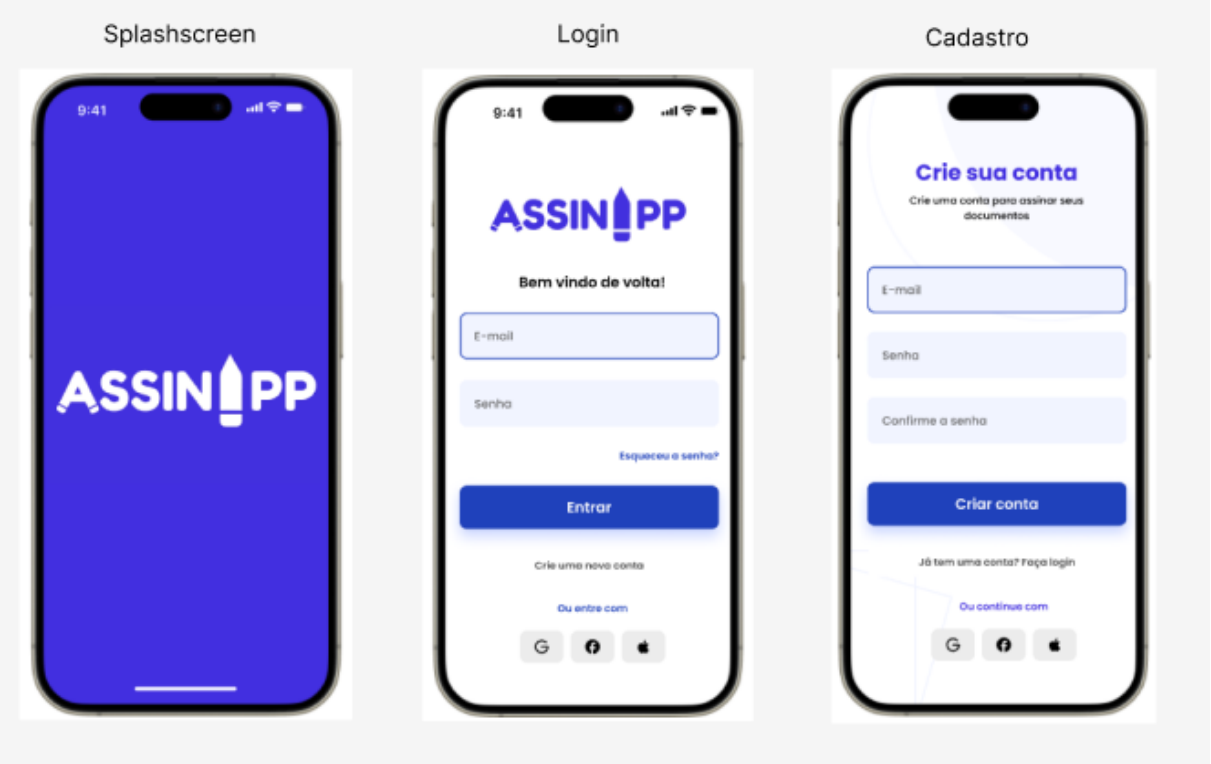
### 5.6.5 Protótipo de Alta Fidelidade

O protótipo de alta fidelidade[4] é ilustrado nas Figuras 23, 24 e 25 e apresenta uma visualização detalhada da interface do aplicativo, garantindo que o design final esteja alinhado às expectativas de usabilidade e acessibilidade. O protótipo foi desenvolvido utilizando a ferramenta Figma, permitindo a criação de interações e fluxos realistas antes da implementação definitiva.

[2] Disponível em: <https://fonts.google.com/specimen/Fredoka>. Acesso em: 28 jan. 2025.
[3] Disponível em: <https://fonts.google.com/specimen/Poppins>. Acesso em: 28 jan. 2025.
[4] Disponível em: <https://www.figma.com/design/KdDdm2fyWNQe6OmXb1WGP5/TCC-Assinatura-digital?node-id=0-1&t=J32PFOrP3D3uzYh6-1>. Acesso em: 28 jan. 2025.

### Splashscreen, Login, Registrar

Figura 23 – Splashscreen, Login, Registrar

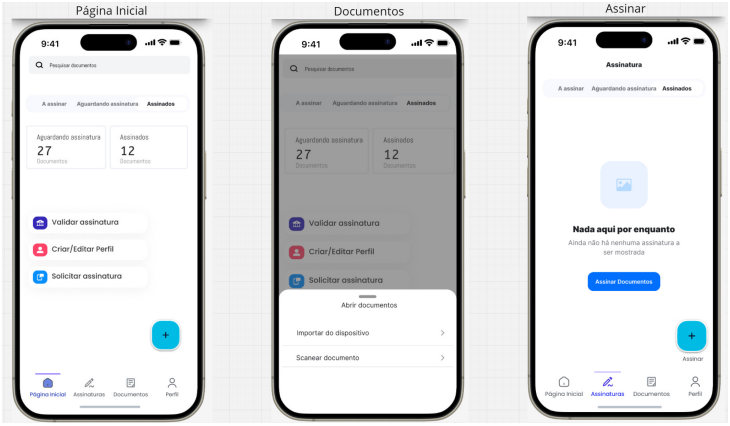



*Fonte: Autor*

- **Splashscreen**: Tela inicial do aplicativo, exibindo o logotipo e uma animação de carregamento para proporcionar uma experiência inicial agradável ao usuário.
- **Login**: Tela onde o usuário insere suas credenciais para acessar sua conta, com opções de recuperação de senha e login rápido.
- **Criar Conta**: Permite o cadastro de novos usuários, oferecendo login social via Google, Facebook e Apple para maior praticidade.

### Página Inicial, Documentos, Assinar

Figura 24 – Página Inicial, Documentos, Assinar

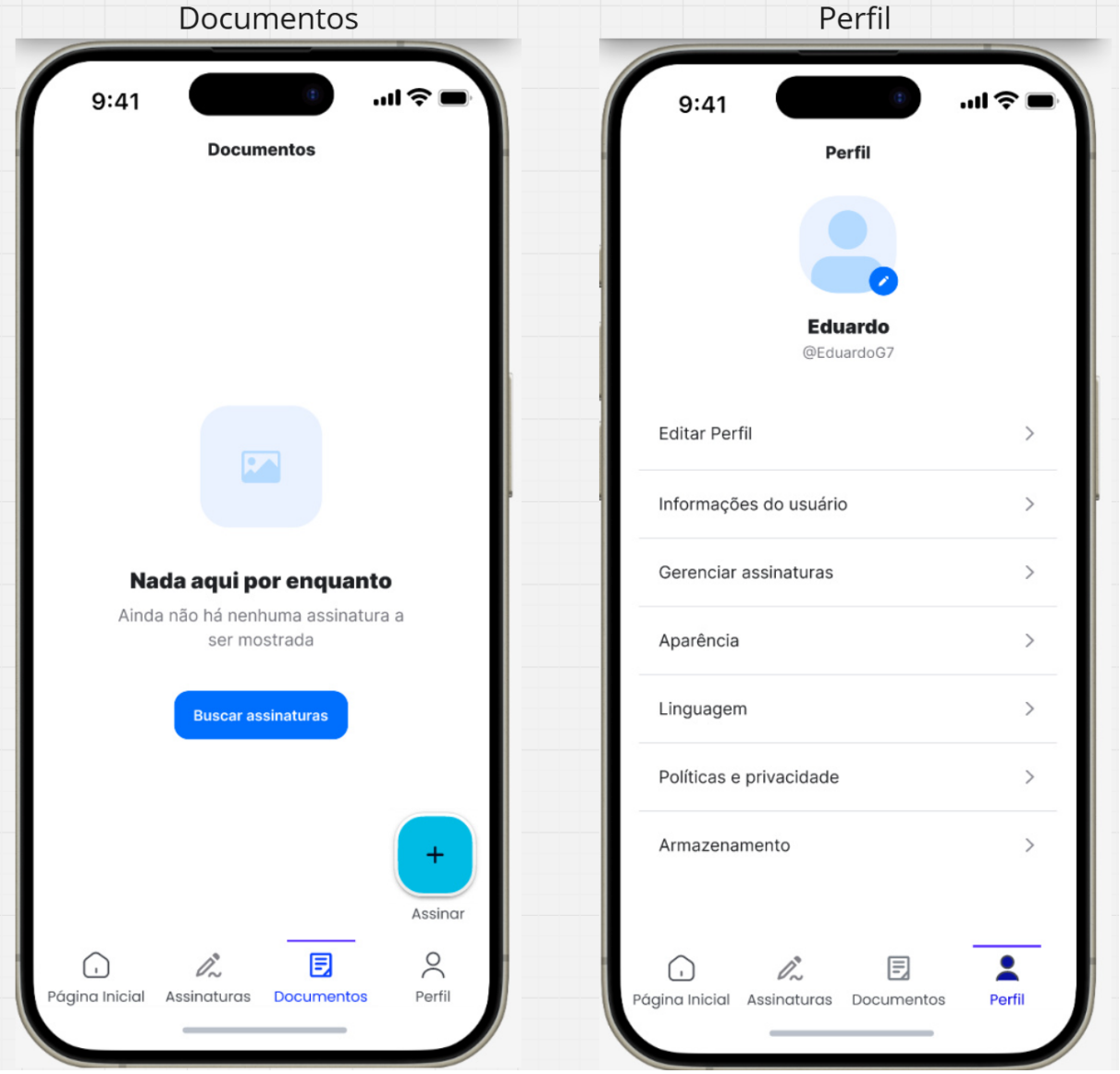



*Fonte: Autor*

- **Página Inicial**: Interface intuitiva com acesso rápido às principais funcionalidades, incluindo validação de assinaturas e gerenciamento de documentos.
- **Tab Assinaturas**: Organização dos documentos em diferentes status (a assinar, aguardando assinaturas e assinados), facilitando o gerenciamento.
- **Modal de Assinatura**: Opção para importar ou escanear documentos diretamente para assinatura.

### Documentos e Perfil

Figura 25 – Documentos e Perfil




*Fonte: Autor*

- **Página de Perfil**: Permite a edição de dados pessoais, configuração de aparência (modo claro/escuro), seleção de idioma, e gerenciamento de assinaturas e armazenamento.

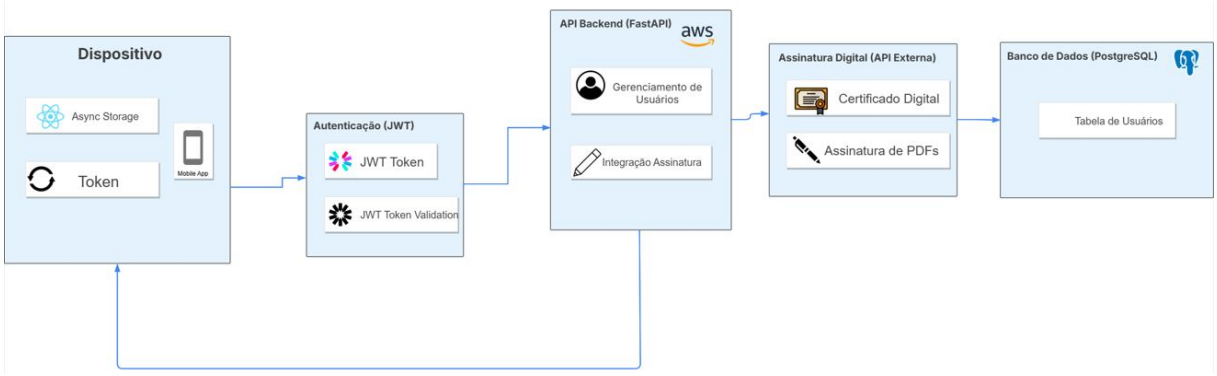
## 5.7 Arquitetura

Nesta seção, detalha-se a arquitetura do aplicativo de assinatura digital, destacando seus componentes principais e como eles se integram para viabilizar as operações do sistema.

### 5.7.1 Visão Geral do Sistema

#### Arquitetura Geral

Figura 26 – Arquitetura Geral




*Fonte: Autor*

A visão geral do sistema, ilustrada na Figura 26, oferece uma descrição abrangente do sistema, destacando seus principais componentes e a forma como eles interagem entre si. Ela ajuda a definir a estrutura básica do sistema, estabelecendo a base para uma melhor compreensão e comunicação entre todos os envolvidos no desenvolvimento do projeto (PRESSMAN, 2014).

No contexto do aplicativo de assinatura digital, a visão geral do sistema abrangeu diferentes camadas, incluindo um aplicativo móvel para interação do usuário, uma API backend responsável pelo processamento das solicitações, um banco de dados para armazenamento estruturado e uma infraestrutura de hospedagem e monitoramento baseada em nuvem.

#### Componentes Principais (atualmente)

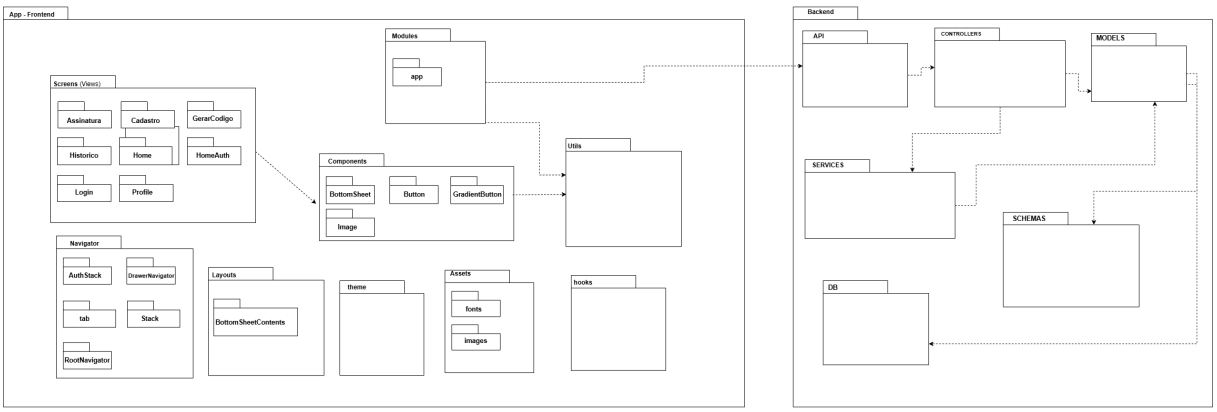
- **Cliente (Frontend)**: O ponto de entrada para o usuário final, implementado com *React Native*. O aplicativo permite aos usuários acessar as funcionalidades do sistema, como autenticação, upload de documentos, e assinatura digital, consumindo os serviços da API backend para processar e armazenar os dados.
- **API Backend (FastAPI)**: O backend da aplicação é responsável por autenticar os usuários, gerenciar seus dados, realizar a assinatura digital e interagir com o banco de dados. Utiliza *FastAPI* para implementar os endpoints e *JWT* para autenticação segura. A API também permite o upload e download de documentos PDF. Toda a infraestrutura do backend está hospedada na *AWS EC2*, garantindo escalabilidade, monitoramento e segurança para o sistema.

- **Assinatura Digital**: O processo de assinatura digital envolve a geração de chaves RSA/ECDSA, que são utilizadas para assinar e verificar os documentos PDF. A API de assinatura digital é chamada pelo backend para garantir a integridade e autenticidade dos documentos.
- **Banco de Dados (PostgreSQL)**: O banco de dados relacional *PostgreSQL* armazena as tabelas de usuários. Ele mantém a integridade e acessibilidade dos dados necessários para o funcionamento do sistema.
- **Armazenamento de Hashes de PDFs**: Os hashes dos documentos PDF são armazenados de forma segura, utilizando o *Async Storage* local para garantir a integridade e controle de versões dos documentos. Esse componente assegura que os documentos sejam versionados e não sejam alterados sem registro.
- **Infraestrutura (AWS EC2)**: O backend do sistema é hospedado na infraestrutura da *AWS EC2*, que garante escalabilidade, monitoramento e segurança. A nuvem também oferece recursos de logs e métricas para acompanhar o desempenho e a utilização da aplicação.

### 5.7.2 Diagrama de Pacotes

**Diagrama de Pacotes**

Figura 27 – Diagrama de Pacotes




*Fonte: Autor*

O diagrama de pacotes, ilustrado na Figura 27, é uma representação visual da estrutura do sistema em termos de pacotes e suas dependências. Ele ajuda a organizar

e modularizar o sistema, facilitando a manutenção e o entendimento das relações entre diferentes partes do código (FOWLER, 2004).

Para o aplicativo de assinatura digital, o diagrama de pacotes mostra como os diferentes módulos estão organizados e interligados, tanto no **front-end** quanto no **back-end**. Isso auxilia na identificação de responsabilidades e na separação de preocupações, garantindo uma arquitetura modular e de fácil manutenção.

#### 5.7.2.1 Front-end

O front-end é responsável pela interface do usuário e pela interação com o sistema. Ele se comunica com o back-end por meio de chamadas HTTP.

- **Pacote de Views (Telas)**: Contém as telas da aplicação, como Login, Cadastro, Assinatura, Histórico e Perfil. Depende dos componentes e serviços para renderizar a interface e buscar dados.
- **Pacote de Components**: Componentes reutilizáveis, como botões, formulários e imagens. Depende de utilitários para funcionalidades auxiliares.
- **Pacote de Services**: Responsável por fazer chamadas HTTP para o back-end, como autenticação, upload de documentos e busca de dados. Depende de utilitários para configurações e funções auxiliares.
- **Pacote de Utils**: Funções utilitárias, como formatação de dados, validações e manipulação de estados.
- **Pacote de Navigator**: Gerencia a navegação entre as telas, como stacks, drawers e tabs.
- **Pacote de Theme**: Define cores, fontes e estilos visuais da aplicação.
- **Pacote de Hooks**: Hooks reutilizáveis para gerenciar estados e efeitos.
- **Pacote de Layouts**: Define layouts comuns, como o conteúdo de bottom sheets.

#### 5.7.2.2 Back-end

O back-end é responsável pela lógica de negócio, processamento de dados e comunicação com o banco de dados.

- **Pacote de API (Endpoints)**: Expõe os endpoints para o front-end, como autenticação, upload de documentos e busca de dados. Depende dos controllers para processar as requisições.

- **Pacote de Controllers**: Recebe as requisições da API, valida os dados e encaminha para os services. Depende dos models e services para manipular dados.
- **Pacote de Models**: Representa a estrutura dos dados no banco de dados. Depende dos schemas para validação e dos services para lógica de negócio.
- **Pacote de Services**: Contém a lógica de negócio, como autenticação, gerenciamento de documentos e notificações. Depende dos models para acessar dados.
- **Pacote de DB (Banco de Dados)**: Gerencia a conexão e operações com o banco de dados.
- **Pacote de Schemas**: Define a estrutura e validação dos dados no banco de dados.

### 5.7.3 Plano de Gerenciamento de Custos

O Gerenciamento do Custo do Projeto envolve processos essenciais para garantir que o projeto seja concluído dentro do orçamento previamente aprovado. Ele inclui etapas como a estimativa de custos, a definição do orçamento e o controle contínuo desses custos. Diversas atividades ao longo do projeto têm impacto financeiro, tornando indispensável o planejamento adequado e o monitoramento rigoroso para manter os gastos sob controle (MORAES, 2012).

#### 5.7.3.1 Custos

O plano de custos do AssinApp foi elaborado considerando fatores relevantes, como os custos relacionados à equipe de desenvolvimento, aquisição de ferramentas e tecnologias, hospedagem de servidores, internet, energia, equipamentos e publicidade.

#### 5.7.3.2 Pessoas

De acordo com a Apuração do Custo das Universidades Federais realizada pelo MEC em 2016, OLIVA (2018), o custo por aluno na Universidade de Brasília (UnB) foi atualizado para considerar a inflação acumulada de 4,83% em 2024. O novo valor corrigido é:

$$R\$54.894,96 \times (1 + 0,0483) = R\$57.547,25$$

Os cálculos detalhados são:

- **Custo diário por aluno:** R$ 57.547,25 / 360 dias ≈ R$ 159,85
- **Custo semanal por aluno:** R$ 159,85 × 6 dias ≈ R$ 959,10

- **Custo semanal para 2 desenvolvedores:** R$ 959,10 × 2 ≈ R$ 1.918,20

O desenvolvimento do AssinApp foi estimado para ser concluído em 12 semanas, resultando em um custo total para a equipe de:

$$R\$1.918,20 \times 12 \text{ semanas} = R\$23.018,40$$

#### 5.7.3.3 Internet

O custo médio de uma internet móvel de 100 GB foi corrigido pela inflação de 4,83%, resultando em:

$$R\$150,00 \times (1 + 0,0483) = R\$157,25$$

Para 3 meses de desenvolvimento:

$$R\$157,25 \times 3 \text{ meses} = R\$471,75$$

#### 5.7.3.4 Energia

O custo médio da energia elétrica no Brasil foi atualizado para incluir a inflação, resultando em um novo valor por kW/h:

$$R\$0,6987 \times (1 + 0,0483) = R\$0,7324$$

O consumo mensal por notebook foi mantido como:

$$\text{Energia mensal por notebook: } 0,03\,\text{kW/h} \times 8\,\text{h/dia} \times 22\,\text{dias} = 5,28\,\text{kW}$$

O custo mensal estimado e atualizado por notebook foi:

$$5,28\,\text{kW} \times R\$0,7324 = R\$3,87$$

Para dois desenvolvedores ao longo de 3 meses, o custo total estimado e atualizado foi:

$$R\$3,87 \times 2\,\text{notebooks} \times 3\,\text{meses} = R\$23,22$$

#### 5.7.3.5 Equipamentos

O custo médio estimado para cada notebook foi atualizado, considerando a inflação:

$$R\$3.509,10 \times (1 + 0,0483) = R\$3.678,49$$

Para dois desenvolvedores, o custo total estimado foi:

$$R\$3.678,49 \times 2 = R\$7.356,98$$

#### 5.7.3.6 Publicidade

Os custos planejados para campanhas publicitárias e taxas de distribuição foram ajustados para refletir a inflação e a taxa de câmbio atualizada. Os valores atualizados foram:

- Anúncios em redes sociais: R$ 2.096,60/mês
- Campanhas de e-mail marketing: R$ 524,15/mês
- Taxa de cadastro na Google Play Store: R$ 144,06 (custo único atualizado).

O custo total estimado e atualizado para 3 meses foi:

$$(R\$2.096,60 + R\$524,15) \times 3 + R\$144,06 = R\$7.886,21$$

#### 5.7.3.7 Hospedagem de Servidores

A hospedagem de servidores é essencial para garantir o funcionamento do AssinApp. Os custos foram calculados considerando serviços da Google Cloud, AWS e Azure, com conversão de valores utilizando a cotação do dólar a R$ 5,79[5]

- **Google Cloud:** Cloud Workstations custa US$ 73,36/mês e a taxa de cluster custa US$ 144,00/mês. Total mensal em reais:

$$(73,36 + 144,00) \times 5,79 = R\$1.257,83$$

- **AWS:** O custo médio de hospedagem é de US$ 1,50/mês. Convertendo:

$$1,50 \times 5,79 = R\$8,69$$

[5] WISE. *Conversor de Moeda*. Disponível em: <https://wise.com/br/currency-converter/dolar-hoje>. Acesso em: 4 fev. 2025.

- **Azure:** Instância A1 custa US$ 58,40/mês. Convertendo:

$$58,40 \times 5,79 = R\$338,14$$

#### 5.7.3.8 Custos da AWS

Foram utilizados três serviços gratuitos da AWS, que fazem parte do AWS Free Usage Tier, válido por 12 meses. Abaixo estão os detalhes desses serviços e os custos que seriam incorridos após o término do período gratuito. Todos os valores apresentados correspondem a uma única instância em execução e foram estimados utilizando a ferramenta oficial da AWS[6].

- **Amazon Elastic Compute Cloud (EC2):**
  - **Uso Gratuito:** 750 horas/mês de instância t2.micro.
  - **Custo após o Free Tier:** US$ 13,39/mês (R$ 77,53).
- **Amazon Elastic Block Store (EBS):**
  - **Uso Gratuito:** 30 GB/mês de armazenamento SSD de uso geral.
  - **Custo após o Free Tier:** US$ 4,56/mês (R$ 26,39).
- **Amazon Virtual Private Cloud (VPC):**
  - **Uso Gratuito:** 750 horas/mês de endereço IPv4 público.
  - **Custo após o Free Tier:** US$ 0,005/hora por endereço IPv4, totalizando US$ 3,75/mês (R$ 21,71).

##### 5.7.3.8.1 Projeção de Custos Futuros

Considerando o término do período gratuito após 12 meses e mantendo como base de valores apenas uma instância em execução, os custos mensais estimados para a AWS foram:

$$\text{Custo mensal da AWS} = R\$77,53\,(\text{EC2}) + R\$26,39\,(\text{EBS}) + R\$21,71\,(\text{VPC}) = R\$125,63$$

Para um período de 12 meses após o free tier, o custo total projetado foi:

$$R\$125,63 \times 12 = R\$1.507,56$$

Esses valores foram incluídos no planejamento financeiro do projeto para garantir a sustentabilidade a longo prazo.

[6] AWS. *Criar Estimativa: Configurar Amazon EC2*. Disponível em: <https://calculator.aws/#/createCalculator/ec2-enhancement>. Acesso em: 4 fev. 2025.

#### 5.7.3.8.2 Justificativa para a Escolha da AWS

A escolha da AWS para hospedar o AssinApp foi baseada no potencial que a plataforma possui para oferecer escalabilidade, permitindo ajuste dinâmico de recursos conforme a demanda, alta confiabilidade, devido à infraestrutura global de data centers, e um suporte técnico eficiente. Além disso, a AWS oferece uma estrutura robusta e flexível, ideal para projetos que podem precisar de expansão no futuro.

### 5.7.3.9 Resumo dos Custos Gerais

Na Tabela 10, apresenta-se um resumo consolidado dos custos do AssinApp, categorizando as principais despesas envolvidas no desenvolvimento e manutenção do projeto. Os valores de hospedagem correspondem a uma única instância em execução.

Tabela 10 – Resumo dos Custos do AssinApp

| **Categoria** | **Custo Total (R$)** |
|---|---:|
| Pessoas | 23.018,40 |
| Internet | 471,75 |
| Energia | 23,22 |
| Equipamentos | 7.356,98 |
| Publicidade | 7.886,21 |
| Hospedagem de Servidores (AWS - Free Tier) | 26,07 |
| Hospedagem de Servidores (AWS - Pós Free Tier) | 1.507,56 |
| **Total Geral** | **40.290,19** |

## 5.8 Considerações Finais do Capítulo

Neste capítulo, foi abordado o desenvolvimento do aplicativo AssinApp, projetado para facilitar a assinatura digital de documentos. Iniciamos com a contextualização da importância da assinatura digital no cenário atual, destacando como essa tecnologia é crucial para garantir a segurança e a autenticidade dos documentos eletrônicos.

O AssinApp foi descrito em detalhes, evidenciando suas principais funcionalidades e como ele se diferencia das soluções existentes. O público-alvo do aplicativo foi identificado e segmentado, com a definição de personas para entender melhor as necessidades dos usuários finais. Em seguida, realizamos um estudo de soluções similares no mercado, analisando ferramentas como GOV.BR, Autentique, Assine PDF, DocuSign e SIGNply. Cada uma dessas ferramentas foi avaliada em termos de funcionalidades, pontos positivos e negativos, permitindo uma comparação abrangente e destacando as áreas onde o AssinApp pode oferecer vantagens.

Os requisitos do AssinApp foram detalhados, incluindo uma explicação dos requisitos funcionais e não funcionais, uma tabela de requisitos que resume as funcionalidades desejadas, e a Estrutura Analítica do Projeto (EAP), que fornece uma visão hierárquica das entregas e atividades do projeto. O protótipo de alta fidelidade foi apresentado para ilustrar as interfaces do usuário e a experiência de interação com o aplicativo.

Por fim, abordamos a arquitetura do AssinApp, incluindo uma visão geral do sistema e o diagrama de pacotes que mostra a organização dos componentes. Além disso, foi elaborado um plano de custos para avaliar os recursos financeiros necessários ao desenvolvimento e manutenção do AssinApp, proporcionando uma visão clara dos investimentos envolvidos.

# 6 Conclusão

Este trabalho buscou desenvolver uma solução prática para a implementação de assinaturas digitais em dispositivos móveis, atendendo às necessidades de segurança e usabilidade dos usuários. Através do processo de desenvolvimento do AssinApp, foram alcançados importantes marcos, como a entrega de um protótipo funcional que realiza o carimbo digital em documentos. Além disso, o aplicativo foi adaptado para integrar uma API que utiliza certificados digitais e a infraestrutura de chave pública (PKI), garantindo a confiabilidade das assinaturas digitais. As fases de pesquisa-ação e os feedbacks dos usuários desempenharam um papel crucial no refinamento contínuo do aplicativo, possibilitando melhorias tanto na usabilidade quanto na segurança da aplicação.

A experiência de desenvolver o AssinApp foi extremamente enriquecedora, pois não apenas permitiu aplicar conhecimentos adquiridos durante a graduação, mas também proporcionou uma compreensão mais profunda dos desafios e oportunidades na implementação de soluções de assinatura digital. Ao interagir com os usuários e integrar suas sugestões, foi possível refinar o produto, o que trouxe uma sensação de propósito e aprendizado contínuo. Além disso, os desafios técnicos, como a integração com a infraestrutura PKI e a busca por uma solução segura e escalável, foram fundamentais para o crescimento e aprimoramento técnicos da dupla autora.

Com base nessa experiência e no processo de busca constante pelo refinamento do aplicativo, este capítulo apresenta as possibilidades de aprimoramento e expansão do AssinApp, considerando tanto as demandas identificadas ao longo do desenvolvimento quanto as sugestões coletadas durante as fases de validação na pesquisa-ação. Com o objetivo de tornar o aplicativo ainda mais robusto, seguro e alinhado às necessidades dos usuários, são propostas funcionalidades adicionais e melhorias contínuas.

Inicialmente, são abordados os Objetivos Concluídos, destacando os resultados alcançados e as metas parcialmente cumpridas. Em seguida, são elencadas as sugestões de Trabalhos Futuros, com foco em funcionalidades que podem ampliar as capacidades do AssinApp, como a integração com a ICP-Brasil e o desenvolvimento de novos recursos voltados à usabilidade e segurança.

## 6.1 Objetivos Concluídos

Retomando os objetivos específicos apresentados no capítulo 1, é possível avaliar o status de cada um conforme o progresso do projeto. A seguir, são detalhados os objetivos e seus respectivos estados de conclusão:

- **Utilizar uma arquitetura de certificados digitais e PKI:** Adotar uma arquitetura existente de certificados digitais e infraestruturas de chave pública (PKI) para garantir a segurança do aplicativo.

  *Status:* Concluído. A arquitetura utilizada foi implementada com base em práticas de segurança recomendadas, fazendo uso de certificados digitais e PKI para garantir a proteção dos dados e a integridade das assinaturas digitais.

- **Implementar o protótipo do aplicativo móvel:** Desenvolver e testar um protótipo funcional do aplicativo móvel, integrando a solução de assinatura digital e garantindo que ele seja intuitivo e fácil de usar.

  *Status:* Concluído. O protótipo está funcional, permitindo o carimbo digital nos documentos. Ajustes de usabilidade foram realizados com base no feedback dos usuários durante as fases da pesquisa-ação. Detalhes sobre o desenvolvimento encontram-se no capítulo 5.

- **Documentar e avaliar a solução:** Elaborar uma documentação detalhada do processo de desenvolvimento, das tecnologias utilizadas e dos resultados obtidos.

  *Status:* Concluído. A documentação do desenvolvimento foi finalizada, incluindo análises detalhadas de desempenho e feedbacks dos usuários. Essa atividade foi concluída com base no ciclo de validação e refinamento do aplicativo.

Foi possível alcançar os objetivos específicos descritos na seção 1.2. A arquitetura existente utilizada foi segura, projetada e implementada com sucesso, garantindo a proteção dos dados e a integridade das assinaturas digitais. O protótipo funcional do aplicativo móvel foi concluído, incluindo ajustes de usabilidade com base no feedback dos usuários. A documentação detalhada do desenvolvimento também foi finalizada, refletindo as análises de desempenho e os feedbacks obtidos durante a pesquisa-ação.

## 6.2 Trabalhos Futuros

Visando aprimorar o AssinApp e atender a novas demandas dos usuários, as seguintes funcionalidades são propostas para futuros desenvolvimentos:

- **Envio de Documentos para Assinatura:** Implementar a funcionalidade de enviar documentos para outros usuários assinarem, ampliando as possibilidades de fluxo de trabalho colaborativo.

- **Assinatura com Rubrica:** Adicionar a opção de assinar com rubrica, oferecendo maior flexibilidade na personalização das assinaturas digitais.

- **Verificação de Assinaturas Existentes:** Permitir a verificação de assinaturas já presentes em documentos, garantindo a autenticidade e integridade das assinaturas digitais.
- **Integração com ICP-Brasil:** Expandir a infraestrutura para suportar a validação das assinaturas conforme os padrões da ICP-Brasil, garantindo conformidade legal e segurança adicional.
- **Suporte a Múltiplos Formatos:** Ampliar o suporte a diversos formatos de documentos, além do PDF, aumentando a versatilidade da aplicação.
- **Possibilitar a compatibilidade multiplataforma:** Verificar e ajustar o protótipo para garantir que ele funcione corretamente tanto em dispositivos iOS quanto Android, utilizando emuladores e testes em dispositivos físicos, quando possível.

# Referências

ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2. ed. Boston: Addison-Wesley, 2003. Citado na página 29.

ALKHALIL, Z. et al. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, Frontiers Media SA, v. 3, p. 563060, 2021. Citado na página 32.

ANDROID. *Android Studio*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://developer.android.com/studio/intro?hl=pt-br>. Citado na página 44.

AWS. *What is Amazon EC2?* 2024. Disponível em: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>. Citado na página 43.

AZEVEDO, L. G. Desenvolvimento de soluções com serviços: Soa, cloud e microsserviços. 2020. Citado na página 35.

AZIZ, O. et al. Research trends in enterprise service bus (esb) applications: A systematic mapping study. *IEEE access*, IEEE, v. 8, p. 31180–31197, 2020. Citado na página 36.

BARBOZA, E. d. S. et al. *Autenticação multifatorial em hardware para o processo de assinatura digital da NF-e*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2018. Citado na página 33.

BASS PAUL CLEMENTS, e. R. K. L. Software architecture in practice. *Addison-Wesley Professional*, v. 2, n. 1, p. 1–16, 2003. Citado na página 79.

BERNARDO, P. C.; KON, F. A importância dos testes automatizados. *Engenharia de Software Magazine*, v. 1, n. 3, p. 54–57, 2008. Citado na página 35.

BINE, J.; KUK, J. N. Estudo de segurança em dispositivos móveis. *Departamento de ciência da computação. Semana acadêmica. Universidade do centro-oeste. UNICENTRO. Guarapuava*, 2016. Citado na página 31.

BIØRN-HANSEN, A.; GRØNLI, T.-M.; GHINEA, G. A survey and taxonomy of core concepts and research challenges in cross-platform mobile development. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 51, n. 5, p. 1–34, 2018. Citado na página 35.

BOEG, J. Kanban em 10 passos. *Tradução de Leonardo Campos, Marcelo Costa, Lúcio Camilo, Rafael Buzon, Paulo Rebelo, Eric Fer, Ivo La Puma, Leonardo Galvão, Thiago Vespa, Manoel Pimentel e Daniel Wildt. C4Media*, p. 27, 2010. Citado na página 52.

Brasil. *Lei nº 10.779, de 14 de setembro de 2003*. [S.l.], 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.779.htm>. Citado na página 59.

BROWN, D. *Designing UX: The Art of Creating the User Experience*. 2. ed. New York: Rosenfeld Media, 2021. Citado na página 36.

CALÇADO, V. L. X. d. S. Influência da utilização de processo unificado, testes e métricas na qualidade de produtos de software. 2007. Citado na página 35.

CENTER, N. C. S. *Trusted network interpretation of the trusted computer system evaluation criteria*. [S.l.]: National Computer Security Center, 1987. v. 5. Citado na página 34.

COMBE, T.; MARTIN, A.; PIETRO, R. D. To docker or not to docker: A security perspective. *IEEE Cloud Computing*, IEEE, v. 3, n. 5, p. 54–62, 2016. Citado na página 36.

CONTI, M.; DRAGONI, N.; LESYK, V. A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, IEEE, v. 18, n. 3, p. 2027–2051, 2016. Citado na página 33.

COOPER, A.; REIMANN, R.; CRONIN, D. *The Inmates Are Running the Asylum*. [S.l.]: Sams Publishing, 1999. Citado na página 60.

COPALO, E. D. R. Icp-brasil. *Revista CEJ*, v. 7, n. 20, p. 58–66, 2003. Citado na página 33.

DOCKER, I. Docker. *línea].[Junio de 2017]. Disponible en: https://www. docker. com/what-docker*, 2020. Citado na página 44.

DORNELES, S. L.; CORRÊA, R. F. Gestão de documentos digitais em aplicações de certificação digital. *Informação arquivística*, v. 2, n. 2, p. 3–31, 2013. Citado na página 33.

ESPINDOLA, R. S. de; MAJDENBAUM, A.; AUDY, J. L. N. Uma análise crítica dos desafios para engenharia de requisitos em manutenção de software. In: *WER*. [S.l.: s.n.], 2004. p. 226–238. Citado na página 36.

European Telecommunications Standards Institute. *Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers issuing certificates; Part 1: General requirements*. 2015. Accessed: 2024-08-12. Disponível em: <https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/02.01.01_60/en_31941101v020101p.pdf>. Citado na página 23.

European Union. *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures*. [S.l.], 1999. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093>. Citado 2 vezes nas páginas 52 e 59.

Expo. *Expo: Desenvolvimento de Aplicativos Móveis*. [S.l.], 2022. Acessado em: 2022-01-01. Disponível em: <https://expo.dev>. Citado na página 44.

EXPO. *Expo DocumentPicker*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://docs.expo.dev/versions/latest/sdk/document-picker/>. Citado na página 45.

FADEL, A. C.; SILVEIRA, H. d. M. Metodologias ágeis no contexto de desenvolvimento de software: Xp, scrum e lean. *Monografia do Curso de Mestrado FT-027-Gestão de Projetos e Qualidade da Faculdade de Tecnologia–UNICAMP*, v. 98, p. 101, 2010. Citado na página 53.

FastAPI. *FastAPI*. 2022. Disponível em: <https://fastapi.tiangolo.com/>. Citado na página 43.

FIGMA. *Protótipo Assinatura Digital no Figma*. 2022. <https://www.figma.com/design/KdDdm2fyWNQe6OmXb1WGP5/TCC-Assinatura-digital?node-id=0-1&t=J32PFOrP3D3uzYh6-1>. Acessado em 03 de setembro de 2024. Citado na página 41.

FLORA, H. K.; WANG, X.; CHANDE, S. V. An investigation into mobile application development processes: Challenges and best practices. *International Journal of Modern Education and Computer Science*, Modern Education and Computer Science Press, v. 6, n. 6, p. 1, 2014. Citado na página 35.

FONSECA, J. J. S. da. *Apostila de metodologia da pesquisa científica*. [S.l.]: João José Saraiva da Fonseca, 2002. Citado na página 50.

FOWLER, M. *UML Distilled: A Brief Guide to the Standard Object Modeling Language*. [S.l.]: Addison-Wesley Professional, 2004. Citado na página 91.

GANDINI, J. A. D.; SALOMÃO, D. P. d. S.; JACOB, C. A segurança dos documentos digitais. *Revista Jurídica: Órgão Nacional de Doutrina, Jurisprudência, Legislação e Crítica Judiciária, Porto Alegre, Ano*, v. 53, p. 59–71, 2001. Citado na página 27.

Gartner. *Market Guide for Digital Signature Solutions*. [S.l.], 2023. Disponível em: <https://www.gartner.com/en/doc/4640495>. Citado na página 52.

GERHARDT, T. E.; SILVEIRA, D. T. *Métodos de pesquisa*. [S.l.]: Plageder, 2009. Citado na página 49.

GIL, A. C. *Como elaborar projetos de pesquisa*. [S.l.]: Editora Atlas SA, 2002. Citado 3 vezes nas páginas 50, 51 e 55.

Git. *Git: Sistema de Controle de Versão*. [S.l.], 2022. Acessado em: 2022-01-01. Disponível em: <https://git-scm.com>. Citado na página 44.

GitHub. *GitHub: Hospedagem de Código-fonte*. [S.l.], 2022. Acessado em: 2022-01-01. Disponível em: <https://github.com>. Citado na página 44.

GOV.BR. *Assinatura Eletrônica GOV.BR*. [S.l.], 2022. Acessado em: 2022-07-28. Disponível em: <https://www.gov.br/governodigital/pt-br/identidade/assinatura-eletronica/assinatura-eletronica-para-orgaos>. Citado 2 vezes nas páginas 52 e 65.

GREENWOOD, D. S. J. S. G.; KHAN, Z. L. L. Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps. In: *Network and Distributed System Security Symposium (NDSS). Internet Society, San Diego, CA*. [S.l.: s.n.], 2014. p. 1–14. Citado na página 33.

HAAS, F. et al. A possibilidade da execução de contratos eletrônicos de direito privado consubstanciados em assinaturas sem a certificação icp-brasil: Uma análise da mp n. 2.200-2/2001 e suas repercussões nas decisões do tribunal de justiça de santa catarina e do superior tribunal de justiça. Florianópolis, SC., 2022. Citado na página 27.

HOUSLEY, R.; POLK, T. *Planning for PKI: best practices guide for deploying public key infrastructure*. [S.l.]: John Wiley & Sons, 2001. Citado 2 vezes nas páginas 23 e 52.

HOUSLEY, R.; POLK, T. *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. [S.l.]: John Wiley & Sons, 2001. Citado na página 29.

HÜHNLEIN, D. Towards eidas as a service. In: SPRINGER. *ISSE 2014 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2014 Conference*. [S.l.], 2014. p. 241–248. Citado na página 35.

Instituto Nacional de Padrões e Tecnologia. *A Digital Signature Standard (DSS)*. 2013. Accessed: 2024-08-12. Disponível em: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>. Citado na página 23.

International Organization for Standardization. *ISO/IEC 27001:2013 - Information security management systems*. [S.l.], 2013. Disponível em: <https://www.iso.org/standard/54534.html>. Citado na página 59.

ISO/IEC. *ISO/IEC 25010:2011 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*. 2011. Acessado em: 29-ago-2024. Disponível em: <https://www.iso.org/standard/35733.html>. Citado na página 79.

JGRAPH LTD. *Draw.io*. [S.l.], 2022. Accessed: 2022-01-01. Disponível em: <https://www.draw.io>. Citado na página 41.

Jira. *Jira: Ferramenta de Gestão de Projetos*. [S.l.], 2022. Acessado em: 2022-01-01. Disponível em: <https://www.atlassian.com/software/jira>. Citado na página 44.

JONES, R. *Efficient Workflow Integration: Best Practices for Digital Systems*. [S.l.]: Workflow Publishing, 2019. Citado na página 36.

KAUFMAN, C.; PERLMAN, R.; SPECINER, M. *Network Security: Private Communication in a Public World*. 2. ed. Upper Saddle River, NJ: Prentice Hall, 2016. Citado na página 29.

KERZNER, H. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*. 13th edition. ed. Hoboken, NJ: John Wiley & Sons, 2022. Citado na página 80.

KOTLIN. *kotlin*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://kotlinlang.org/docs/getting-started.html>. Citado na página 42.

KRUG, S. *Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability*. 3rd edition. ed. [S.l.]: New Riders, 2013. Citado na página 37.

LIPP, e. a. Electronic signatures and infrastructures (esi). *European Telecommunications Standards Institute (ETSI)*, 2012. Citado 2 vezes nas páginas 28 e 52.

LIPP, M. et al. *ETSI Digital Signature Standard*. Sophia-Antipolis, France, 2012. Accessed: 2024-08-30. Disponível em: <https://www.etsi.org/deliver/etsi_ts/102700_102799/102778/01.01.01_60/ts_102778v010101p.pdf>. Citado na página 52.

LUCID SOFTWARE INC. *LucidChart*. [S.l.], 2022. Accessed: 2022-01-01. Disponível em: <https://www.lucidchart.com>. Citado na página 41.

MACIEL, H. *Assinatura Digital*. 2008. Acesso em: 31 ago. 2024. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/Anos-anteriores/2008-2/trabalhos_vf/hugo/AssinaturaDigital.html>. Citado na página 28.

MACIEL, R. d. S. *Avaliação do impacto de ataques DDoS e Malware: uma abordagem baseada em árvore de ataque*. Dissertação (Mestrado) — Universidade Federal de Pernambuco, 2018. Citado na página 32.

MAXIM, R. S. P. e B. R. *Software Engineering: A Practitioner's Approach*. 9ª. ed. New York, NY, USA: McGraw-Hill Education, 2020. Citado na página 79.

MELAMED, T. An active man-in-the-middle attack on bluetooth smart devices. *Safety and Security Studies*, WIT Press, v. 15, p. 2018, 2018. Citado na página 33.

MENKE, F. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a icp alemã. *Revista de direito do consumidor*, v. 12, n. 48, p. 17, 2003. Citado na página 35.

MODELER. *Bizagi Modeler*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://help.bizagi.com/platform/en/index.html?creating_a_documentation_porta.htm>. Citado na página 42.

MORAES, E. A. P. Guia pmbok para gerenciamento de projetos. In: SN. *Anais do Congresso Nacional de Excelência em Gestão, Rio de Janeiro, RJ, Brasil*. [S.l.], 2012. v. 8. Citado na página 92.

NIELSEN, J. *Designing User Interfaces for High-Impact Digital Products*. [S.l.]: Nielsen Norman Group, 2020. Citado 2 vezes nas páginas 36 e 37.

NOGUEIRA, T. et al. Diretrizes de acessibilidade na web e redes sociais: Uma revisao sistemática da literatura. In: SBC. *Anais do VIII Workshop sobre Aspectos da Interação Humano-Computador para a Web Social*. [S.l.], 2017. p. 70–81. Citado na página 81.

NORMAN, D. *The Design of Everyday Things*. Revised and expanded edition. [S.l.]: Basic Books, 2013. Citado na página 37.

NPM. *token jsonweb*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://www.npmjs.com/package/jsonwebtoken>. Citado na página 45.

OLIVA, P. Apuração do custo das universidades federais e sua relação com os respectivos quantitativos de alunos. *Nota Técnica MEC/SE*, n. 4, 2018. Citado na página 92.

ORACLE. *Java*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://docs.oracle.com/en/java/>. Citado na página 42.

OTTONI, M. B. Certificação digital e segurança. *São Paulo: Certisign*, 2005. Citado na página 31.

Overleaf. *Overleaf: Ferramenta de Edição de Documentos LaTeX*. [S.l.], 2022. Acessado em: 2022-01-01. Disponível em: <https://www.overleaf.com>. Citado na página 45.

PostgreeSQL. *PostgreeSQL*. 2024. Disponível em: <https://www.postgresql.org/docs/>. Citado na página 43.

PRESSMAN, R. S. *Software Engineering: A Practitioner's Approach*. [S.l.]: McGraw-Hill Education, 2014. Citado na página 89.

PUB, F. Digital signature standard (dss). *Fips pub*, p. 186–192, 2000. Citado na página 52.

PYTHON. *Python*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://docs.python.org/pt-br/3/tutorial/index.html>. Citado na página 43.

RAMZAN, Z. Phishing attacks and countermeasures. *Handbook of information and communication security*, Springer, p. 433–448, 2010. Citado na página 31.

React Native. *React Native: Mobile App Development Framework*. 2022. Disponível em: <https://reactnative.dev/>. Citado na página 42.

REACT NATIVE. *React Native PDF*. [S.l.], 2024. Accessed: 2025-01-25. Disponível em: <https://www.npmjs.com/package/react-native-pdf>. Citado na página 44.

SANTOS, A. d. S. d. Auditoria de sistemas de desenvolvimento de software. 004, 2014. Citado na página 35.

SANTOS, H. M. dos; FLORES, D. Preservação de documentos arquivísticos digitais autênticos: reflexões e perspectivas. 2015. Citado na página 27.

SCHWABER, K.; SUTHERLAND, J. The scrum guide. *Scrum Alliance*, v. 21, n. 1, p. 1–38, 2011. Citado na página 52.

SHNEIDERMAN, B. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 6. ed. Boston: Addison-Wesley, 2016. Citado na página 37.

SMITH, L. *Designing for Accessibility: A Guide for UX Professionals*. [S.l.]: Apress, 2020. Citado na página 38.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 4th edition. ed. [S.l.]: Prentice Hall, 2006. Citado 2 vezes nas páginas 29 e 52.

STALLINGS, W. *Criptografia e segurança de redes: Princípios e práticas*. 6. ed. São Paulo: Pearson, 2017. Citado 2 vezes nas páginas 28 e 30.

STANDARDS, N. I. of; (NIST), T. *Digital Signature Standard (DSS)*. [S.l.], 2000. NIST PUB. Citado na página 28.

THE OPENSSL PROJECT. *OpenSSL*. [S.l.], 2022. Accessed: 2022-01-01. Disponível em: <https://www.openssl.org>. Citado na página 42.

THIOLLENT, M. *Metodologia da pesquisa-ação*. [S.l.]: Cortez editora, 2022. Citado 2 vezes nas páginas 50 e 55.

TOLMASQUIM, M. T. Perspectivas e planejamento do setor energético no brasil. *Estudos avançados*, SciELO Brasil, v. 26, p. 247–260, 2012. Citado na página 23.

VITAL, L. P. O pdf/a na gestão de documentos arquivísticos. *ÁGORA: Arquivologia em debate*, v. 21, n. 43, p. 73–79, 2011. Citado na página 27.

(WAI), W. A. I. *Web Content Accessibility Guidelines (WCAG) 2.1*. [S.l.], 2018. Acesso em: 31 ago. 2024. Disponível em: <https://www.w3.org/TR/WCAG21/>. Citado na página 38.

YOU, I.; YIM, K. Malware obfuscation techniques: A brief survey. In: IEEE. *2010 International conference on broadband, wireless computing, communication and applications*. [S.l.], 2010. p. 297–300. Citado na página 32.

ZHANG, W.; LI, X. Challenges and opportunities in mobile app development. *IEEE Computer*, v. 43, n. 4, p. 34–39, 2010. Citado na página 23.