

Ferramentas para integração de informação médica

Lucas Teixeira Rocha

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática
(2º ciclo de estudos)

Orientador: Prof. Doutor Paulo Fazendeiro
Co-orientador: Prof. Doutor Francisco Morgado

Junho de 2025

Declaração de Integridade

Eu, Lucas Teixeira Rocha, que abaixo assino, estudante com o número de inscrição M11813 do Mestrado em Engenharia Informática da Faculdade de Engenharia, declaro ter desenvolvido o presente trabalho e elaborado o presente texto em total consonância com o Código de Integridades da Universidade da Beira Interior.

Mais concretamente afirmo não ter incorrido em qualquer das variedades de Fraude Académica, e que aqui declaro conhecer, que em particular atendi à exigida referência de frases, extratos, imagens e outras formas de trabalho intelectual, e assumindo assim na íntegra as responsabilidades da autoria.

Universidade da Beira Interior, Covilhã 04/06/2025

Dedicatória

Dedico este trabalho aos meus queridos pais, **Mayra** e à memória de **Jorge**, cujos ensinamentos e exemplos de vida sempre foram minha inspiração.

À minha esposa, **Renata**, por sua paciência, amor e apoio incondicional.

E às minhas filhas, **Laura** e **Mariana**, que iluminam minha vida com alegria e motivam cada passo do meu caminho.

Agradecimentos

Gostaria de expressar minha sincera gratidão aos meus orientadores, **Dr. Paulo Fazendeiro** e **Dr. Francisco Morgado**, pelo suporte técnico, orientação acadêmica e pela dedicação ao longo de todo o processo de desenvolvimento deste trabalho. Ao Instituto de Telecomunicações (Delegação da Covilhã) pelo acolhimento durante parte do tempo dedicado à realização dos trabalhos de desenvolvimento.

Agradeço também aos meus irmãos — Iury, Ian, Neill, Lin e Isaac — e à minha irmã, Luísa, pelo apoio emocional e pelas palavras de encorajamento, que foram fundamentais nos momentos mais desafiadores.

Por fim, um agradecimento especial a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, oferecendo suporte, inspiração e motivação.

Prefácio

O presente trabalho representa o culminar de um esforço acadêmico e pessoal dedicado à compreensão e aplicação de tecnologias que possam transformar a gestão de informações de saúde. Ao longo desta jornada, foram enfrentados desafios técnicos, intelectuais e pessoais, que contribuíram significativamente para o amadurecimento não apenas como profissional, mas também como ser humano.

A motivação para este projeto surgiu da constatação de como a integração de tecnologias modernas pode impactar positivamente a vida de utentes e profissionais de saúde, promovendo uma interação mais eficiente e humanizada. Neste contexto, a combinação de ferramentas como *e-Health*, computação móvel e padrões de interoperabilidade tem o potencial de atender às demandas crescentes do setor de saúde digital.

Este trabalho não seria possível sem o apoio de muitas pessoas e instituições. A dedicação e o suporte dos meus orientadores, familiares, colegas e amigos foram essenciais para superar os obstáculos ao longo do caminho. A todos eles, meu sincero agradecimento.

Espero que este trabalho possa servir de base para futuras pesquisas e inspire novas iniciativas que continuem a explorar o uso da tecnologia para melhorar a qualidade de vida das pessoas.

Lucas Teixeira Rocha
Covilhã, 04/06/2025

Resumo

Este trabalho apresenta o desenvolvimento de uma aplicação voltada para a gestão integrada de informações de saúde, com foco na melhoria do acompanhamento de utentes e na facilitação da comunicação entre utentes e profissionais de saúde. A solução utiliza tecnologias modernas, como **Angular** para o frontend e **Firebase** como serviço backend-as-a-service (BaaS), visando oferecer uma interface intuitiva e funcionalidades robustas para cadastro, edição e compartilhamento de informações médicas.

Foram implementadas medidas de segurança, como **criptografia de ponta a ponta** e **logs de auditoria**, para garantir a privacidade e a proteção dos dados sensíveis, atendendo às regulamentações **HIPAA**, **GDPR** e **LGPD**.

Os resultados deste projeto destacam a relevância de ferramentas digitais no contexto de *e-Health*, promovendo uma gestão mais eficiente e acessível das informações de saúde. Espera-se que a aplicação desenvolvida possa contribuir para a melhoria da qualidade do cuidado oferecido, a personalização de tratamentos e a continuidade do acompanhamento clínico, além de abrir caminhos para futuras inovações no setor.

Palavras-chave

e-Health, Interoperabilidade, Segurança da Informação, Serverless.

Abstract

This work presents the development of an application aimed at the integrated management of health information, focusing on improving user follow-up and facilitating communication between users and healthcare professionals. The solution leverages modern technologies, such as **Angular** for the frontend and **Firebase** as a backend-as-a-service (BaaS), to provide an intuitive interface and robust functionalities for registering, editing, and sharing medical information.

Security measures, including **end-to-end encryption** and **audit logs**, were implemented to ensure the privacy and protection of sensitive data, complying with **HIPAA**, **GDPR**, and **LGPD** regulations.

The results of this project highlight the relevance of digital tools in the *e-Health* context, promoting a more efficient and accessible management of health information. The developed application is expected to contribute to improving the quality of care provided, personalizing treatments, and ensuring continuity of clinical follow-up, while paving the way for future innovations in the healthcare sector.

Keywords

e-Health, Information Security, Interoperability, Serverless.

Índice

1	Introdução	1
1.1	Objetivos	1
1.2	Contextualização	1
1.3	Problema Identificado	2
1.4	Solução Proposta	3
2	Revisão Bibliográfica	5
2.1	e-Health e Computação Móvel	5
2.2	Segurança da Informação em Saúde	6
2.2.1	Health Insurance Portability and Accountability Act (HIPAA)	7
2.2.2	General Data Protection Regulation (GDPR)	7
2.2.3	Lei Geral de Proteção de Dados Pessoais (LGPD)	8
2.3	Interoperabilidade entre Sistemas de Saúde	9
2.4	Diretrizes de Usabilidade e Acessibilidade	10
2.5	Aplicações Existentes no Mercado	11
2.6	Inteligência Artificial em e-Health	13
3	Seleção de Metodologias e Tecnologias	15
3.1	Frontend com Angular e Material	15
3.2	Firebase: Hosting, Authentication e Firestore	16
3.2.1	Firebase Hosting	16
3.2.2	Firebase Authentication	17
3.2.3	Cloud Firestore	17
3.2.4	Conclusão	18
3.3	Análise Crítica das Tecnologias Adotadas	18
3.3.1	Frontend com Angular e Material	18
3.3.2	Firebase	19
3.3.3	Conclusão	19
3.4	Uso de Progressive Web App (PWA)	20
3.4.1	Características Principais de PWA	20
3.4.2	Vantagens de Utilizar PWA	20
3.4.3	PWA no Contexto da Aplicação	21
3.5	Versionamento de Código com Git e GitHub	21
3.5.1	Funcionalidades do Git e GitHub	21
3.5.2	Importância para o Projeto	22
3.6	Boas Práticas em DevOps	22
3.6.1	Integração Contínua (CI)	23
3.6.2	Entrega Contínua (CD)	23
3.6.3	GitHub Actions	23

3.6.4	Importância para o Projeto	24
3.7	Metodologias Utilizadas para Gerir Tarefas	24
3.7.1	Metodologias Ágeis e sua Importância	24
3.7.2	Trello e Quadro Kanban	25
4	Padrões e Diretrizes de Segurança	29
4.1	Privacidade dos Dados	29
4.1.1	Conformidade com Regulamentações	29
4.1.2	Medidas de Segurança	29
4.1.3	Importância das Medidas de Privacidade	31
4.2	Gestão de Segurança da Informação em Saúde	32
4.2.1	ISO 27001: Base para a Gestão da Segurança da Informação	32
4.2.2	ISO 27799: Foco em Dados de Saúde	32
4.2.3	Complementaridade entre ISO 27799 e ISO 27001	33
4.2.4	Importância da Implementação	33
4.3	Interoperabilidade com Padrões de Saúde	33
4.3.1	HL7 FHIR: Padrão para Interoperabilidade	33
4.3.2	Benefícios da Interoperabilidade com HL7 FHIR	33
4.3.3	Implementação e Desafios	34
5	Implementação e Testes	35
5.1	Implementação da Prova de Conceito	35
5.1.1	Restrição de Acesso com Base na Autenticação e no Papel do Utilizador	35
5.1.2	Cifragem/Decifragem das Informações	37
5.1.3	Logs de Auditoria	38
5.1.4	Restrição de Acesso aos Dados de Utentes	39
5.2	Testes de Usabilidade	41
5.2.1	Resultados Quantitativos	41
5.2.2	Resultados Qualitativos	41
5.2.3	Análise dos Resultados	41
6	Trabalhos Futuros e Conclusões	43
6.1	Trabalhos Futuros	43
6.1.1	Gamificação e Incentivos Comportamentais	43
6.1.2	Integração com Dispositivos de IoT	44
6.1.3	Suporte a Dispositivos Médicos de Imagem via DICOM	44
6.1.4	Adição de um Backend Dedicado com Suporte a HL7 FHIR	44
6.1.5	Exploração de Tecnologias Emergentes	45
6.1.6	Testes Automatizados: Unit Tests, E2E e Mutation Testing	45
6.1.7	Resumo dos Próximos Passos	47
6.2	Conclusões	48
	Bibliografia	49

A	Anexos	51
A.1	Requisitos do Sistema	51
A.1.1	Gerenciamento de Utilizadores	51
A.1.2	Funcionalidades para Utentes	51
A.1.3	Funcionalidades para Profissionais de Saúde	52
A.1.4	Notificações	52
A.1.5	Requisitos Não Funcionais	52
A.2	Cronograma de Desenvolvimento	52
A.3	Representações Gráficas dos Resultados dos Testes de Usabilidade	54

Lista de Figuras

3.1	Arquitetura do Angular	15
3.2	Funcionamento de Aplicação com Firebase	17
3.3	Quadro Kanban no Trello	26
4.1	Informações Criptografadas no Firestore	30
4.2	Criptografia AES	31
5.1	Logs de Auditoria	38
5.2	Visualização de Acessos às Informações do Utente	40
6.1	Firebase vs. Aplicação web tradicional	45
A.1	Cronograma de Desenvolvimento - Diagrama de Gantt	53
A.2	Em que tipo de dispositivo utilizou a aplicação?	54
A.3	Por quanto tempo utilizou a aplicação?	54
A.4	Quão fácil e intuitiva foi a utilização da aplicação?	55
A.5	Que nota daria ao design da aplicação?	55
A.6	Que nota daria à qualidade técnica da aplicação?	56
A.7	A aplicação facilitou o acompanhamento e execução do tratamento?	56
A.8	Qual a eficácia da aplicação na gestão das suas informações?	57
A.9	Qual a eficácia da aplicação no partilhamento das suas informações com profissionais de saúde?	57
A.10	Qual o seu nível de confiança na segurança e privacidade das suas informações na aplicação?	58
A.11	Eficácia da aplicação no acompanhamento de utentes.	58
A.12	Nível de confiança na segurança e privacidade das informações dos utentes.	59

Lista de Tabelas

2.1	Tabela Comparativa entre HIPAA, GDPR e LGPD	6
2.2	Tabela Comparativa de Aplicações de e-Health	13
A.1	Cronograma de Desenvolvimento	53

Lista de Acrónimos

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
AWS	Amazon Web Services
BaaS	Backend-as-a-Service
CI/CD	Continuous Integration/Continuous Delivery
DICOM	Digital Imaging and Communications in Medicine
FHIR	Fast Healthcare Interoperability Resources
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
NIST	National Institute of Standards and Technology
PHI	Protected Health Information
PWA	Progressive Web App
RBAC	Role-Based Access Control
SGSI	Sistema de Gestão de Segurança da Informação
SPA	Single-Page Application
TLS	Transport Layer Security
WCAG	Web Content Accessibility Guidelines

Capítulo 1

Introdução

1.1 Objetivos

O principal objetivo deste projeto é desenvolver uma solução integrada que permita ao doente crônico participar ativamente na gestão de suas informações de saúde, enquanto facilita o acesso dessas informações por profissionais de saúde, incluindo médicos, farmacêuticos e outros cuidadores envolvidos no seu tratamento. Para alcançar esse objetivo geral, foram definidos os seguintes objetivos específicos:

- **Integrar informação de saúde de múltiplas fontes:** Agregar dados relacionados à medicação, alergias, sintomas, parâmetros analíticos e outros domínios de saúde, provenientes de diversas fontes, e apresentá-los de forma clara e acessível tanto para o utente quanto para os profissionais de saúde envolvidos no seu acompanhamento.
- **Desenvolver uma aplicação móvel e uma aplicação web seguras:** Criar interfaces digitais que permitam o acesso seguro às informações sensíveis de saúde do usuário, respeitando os mais rigorosos padrões de segurança e privacidade, como o GDPR e a HIPAA, garantindo o controle de acesso e proteção dos dados pessoais.
- **Fomentar a integração entre doente e profissionais de saúde:** Facilitar a comunicação e a troca de informações relevantes entre utentes e profissionais de saúde, promovendo um acompanhamento mais próximo e eficiente do doente crônico, seja no sistema de saúde público, privado ou em farmácias.

Esses objetivos visam fornecer uma solução inovadora, que não só aumenta a eficiência da gestão de informações de saúde, mas também atribui um papel mais ativo ao utente no controle de sua saúde.

1.2 Contextualização

A gestão integrada de informações de saúde desempenha um papel essencial no tratamento de utentes, especialmente no caso de doentes crônicos, que demandam acompanhamento contínuo e frequentemente interagem com diversos profissionais de saúde. Estes utentes, que convivem com condições de longo prazo, geralmente necessitam de monitoramento constante de múltiplos parâmetros de saúde, como medicação, sintomas, sinais vitais e parâmetros laboratoriais. A integração eficiente dessas informações em uma plataforma acessível por todos os profissionais envolvidos no tratamento é fundamental para garantir a continuidade do cuidado e evitar duplicidade de intervenções ou tratamentos contraditórios.

Atualmente, um dos maiores desafios enfrentados pelos sistemas de saúde é a fragmentação das informações entre diferentes instituições e profissionais. Dados sobre o utente muitas vezes estão dispersos entre hospitais, clínicas e farmácias, dificultando a criação de um panorama completo sobre o estado de saúde do indivíduo [1]. A falta de comunicação entre sistemas de saúde público e privado, assim como entre diferentes especialidades, pode resultar em tratamentos incompletos ou até mesmo prejudiciais, como a prescrição de medicamentos que interagem de forma negativa com aqueles já utilizados pelo utente.

Além disso, a participação ativa do utente na gestão de sua própria saúde tem sido amplamente promovida como um fator crucial para o sucesso terapêutico. Quando o utente tem acesso a suas informações de saúde e pode atualizá-las diretamente, como no caso de sintomas e reações a medicamentos, os profissionais de saúde podem reagir de forma mais rápida e precisa às necessidades emergentes do tratamento [3]. Esse fluxo contínuo de informações permite uma maior personalização do tratamento e uma melhor resposta às condições em evolução.

Diante desse cenário, surge a necessidade de ferramentas que integrem os dados provenientes de diferentes fontes, como sistemas hospitalares, registros de farmácias e informações fornecidas diretamente pelo utente. Ao promover essa integração, é possível melhorar significativamente a qualidade do tratamento, otimizar o uso dos recursos de saúde e empoderar o utente para que ele tenha um papel mais ativo na gestão de sua condição.

1.3 Problema Identificado

Os sistemas de saúde contemporâneos enfrentam uma série de desafios relacionados à gestão eficiente de dados clínicos. Um dos principais problemas é o **armazenamento fragmentado de informações** dos utentes, que resulta na dispersão de dados entre diferentes sistemas e instituições de saúde. Muitas vezes, as informações de um único utente são mantidas separadamente por hospitais, clínicas, farmácias e outros serviços, sem que haja uma comunicação eficaz entre essas plataformas. Essa fragmentação impede que os profissionais de saúde acessem um histórico completo e atualizado do utente, o que compromete a continuidade do cuidado [1].

A **falta de integração entre plataformas de saúde públicas e privadas** também agrava essa situação. Em muitos países, os sistemas de saúde públicos e privados operam de forma isolada, com pouca ou nenhuma troca de informações sobre os utentes que transitam entre esses dois sistemas. Essa desconexão impede que médicos e outros profissionais de saúde tenham uma visão holística das condições e tratamentos anteriores do utente, levando a decisões baseadas em informações incompletas [1]. Um exemplo recorrente desse problema é o acompanhamento de doentes crônicos que, muitas vezes, recebem prescrições e diagnósticos em diferentes redes de saúde, sem que os dados sejam consolidados em um único prontuário acessível por todos os cuidadores envolvidos no tratamento.

Além disso, o uso de diferentes formatos de dados e sistemas proprietários cria uma barreira significativa para a interoperabilidade. Sem a adoção de padrões universais de troca de informações, como o HL7 FHIR, as plataformas de saúde permanecem isoladas, resultando

em redundância de exames, erros de medicação e custos elevados para o sistema de saúde [4]. Assim, torna-se imperativo encontrar soluções que promovam a integração desses sistemas, a fim de melhorar a qualidade do cuidado e a eficiência operacional no setor da saúde.

1.4 Solução Proposta

Diante dos desafios apresentados pela fragmentação de dados e pela falta de integração entre plataformas de saúde, a solução proposta visa o desenvolvimento de uma **aplicação móvel e web segura**. O principal objetivo dessa aplicação é facilitar a comunicação entre utentes e profissionais de saúde, ao mesmo tempo em que integra informações relevantes sobre a saúde do utente de forma eficiente e acessível. Essa ferramenta permite que os utentes registrem informações críticas, como medicações, sintomas, alergias e parâmetros vitais, e que esses dados sejam compartilhados em tempo real com os profissionais responsáveis por seu tratamento.

A aplicação proposta foi construída com um enfoque na **segurança dos dados**, garantindo que todas as informações de saúde sejam protegidas de acordo com as regulamentações vigentes, como o **Regulamento Geral sobre a Proteção de Dados (GDPR)** na Europa e a **Health Insurance Portability and Accountability Act (HIPAA)** nos Estados Unidos. Isso inclui a implementação de logs, métodos seguros de autenticação, além de criptografia de ponta a ponta para garantir que os dados estejam protegidos tanto em repouso quanto em trânsito [2].

Além disso, a aplicação foi projetada para suportar o **controle e partilhamento** com profissionais de saúde das informações de saúde existentes. Isso permite que os dados inseridos pelos utentes sejam facilmente acessíveis por médicos, farmacêuticos e outros profissionais, promovendo um cuidado mais coordenado e eficiente. A solução proposta também fomenta a participação ativa dos utentes em seu próprio cuidado, fornecendo a eles uma visão abrangente e centralizada de seus dados de saúde, o que pode contribuir para uma melhor adesão ao tratamento e para melhores desfechos clínicos [3].

Portanto, esta aplicação não apenas resolve os problemas de integração de dados, mas também promove uma **melhor comunicação e participação ativa do utente**, o que é fundamental para o gerenciamento de doenças crônicas e o acompanhamento contínuo.

Capítulo 2

Revisão Bibliográfica

2.1 e-Health e Computação Móvel

A evolução das tecnologias móveis e dos sistemas de **e-Health** tem revolucionado a maneira como os doentes crônicos são acompanhados e gerenciados. O termo **e-Health** refere-se ao uso de tecnologias digitais e de comunicação para melhorar o atendimento à saúde, promovendo o acesso a informações de saúde de forma mais eficiente e segura. Nos últimos anos, a combinação de plataformas móveis e **e-Health** tem desempenhado um papel crucial no cuidado de utentes que necessitam de acompanhamento contínuo, especialmente os que sofrem de doenças crônicas [4].

As tecnologias móveis, como smartphones e tablets, permitem que os utentes se envolvam mais ativamente na gestão de sua própria saúde. Com a popularização de aplicativos móveis dedicados à saúde, os utentes podem monitorar suas condições, registrar sintomas, controlar a medicação e até mesmo receber lembretes de consultas e exames. Além disso, essas aplicações possibilitam que os dados dos utentes sejam compartilhados em tempo real com profissionais de saúde, permitindo um acompanhamento mais ágil e assertivo [4].

Para os doentes crônicos, essa conectividade oferecida pela computação móvel traz inúmeros benefícios. utentes com diabetes, hipertensão e outras doenças de longo prazo podem monitorar seus parâmetros vitais e enviar os resultados diretamente para seus médicos. Isso não apenas facilita um acompanhamento mais frequente, mas também pode alertar os profissionais de saúde sobre alterações que possam requerer intervenção imediata. O uso de **e-Health** nesse contexto reduz a necessidade de visitas presenciais constantes, otimizando os recursos de saúde e melhorando a qualidade de vida dos utentes [4].

Outro benefício significativo é a capacidade dos profissionais de saúde de acompanhar a adesão dos utentes ao tratamento prescrito. Aplicativos móveis podem fornecer lembretes de medicação, enquanto os dados sobre a ingestão de medicamentos podem ser automaticamente registrados e revisados pelos médicos. Isso é particularmente útil para utentes que sofrem de condições que exigem medicação regular e rigorosa, como a insuficiência cardíaca ou a asma.

Com a integração crescente entre **e-Health** e dispositivos móveis, surge a oportunidade de transformar a maneira como os utentes crônicos são monitorados e tratados, promovendo um cuidado mais contínuo, personalizado e proativo. Além disso, o desenvolvimento de novas tecnologias, como a **Internet of Things (IoT)**, promete levar essa integração a um novo patamar, permitindo que dispositivos médicos conectados capturem e transmitam dados de forma automática e em tempo real.

2.2 Segurança da Informação em Saúde

A segurança da informação em saúde é uma prioridade fundamental na era digital, especialmente devido à crescente utilização de tecnologias móveis e plataformas **e-Health**. O gerenciamento seguro de dados sensíveis de utentes, como histórico médico, informações de medicação e parâmetros vitais, requer a adesão a padrões rigorosos de privacidade e proteção de dados. Regulações como a **Health Insurance Portability and Accountability Act (HIPAA)**, o **General Data Protection Regulation (GDPR)** e a **Lei Geral de Proteção de Dados (LGPD)** desempenham um papel crucial para garantir que os dados de saúde sejam armazenados e processados de maneira segura, protegendo a privacidade dos utentes [2].

Além desses requisitos normativos, a adoção de **autenticação de dois fatores (2FA)** é cada vez mais comum para garantir que apenas indivíduos autorizados possam acessar sistemas que contêm dados sensíveis. Combinado com técnicas avançadas de criptografia, o **2FA** ajuda a mitigar o risco de acessos não autorizados, reduzindo significativamente a probabilidade de violações de segurança [2].

Dessa forma, o cumprimento de normas como a **HIPAA**, **GDPR** e **LGPD** não apenas protege a privacidade dos utentes, mas também garante que as organizações de saúde adotem as melhores práticas de segurança, proporcionando um ambiente mais seguro para o gerenciamento de informações sensíveis. A Tabela 2.1 sintetiza uma análise comparativa entre as três regulações.

Tabela 2.1: Tabela Comparativa entre HIPAA, GDPR e LGPD

Aspecto	HIPAA	GDPR	LGPD
Jurisdição	Estados Unidos	União Europeia	Brasil
Tipo de Dados Protegidos	Informações de Saúde (PHI - Protected Health Information)	Dados Pessoais	Dados Pessoais
Consentimento do Titular	Necessário para o compartilhamento de informações, com algumas exceções para tratamento e operações	Deve ser livre, informado e explícito	Deve ser livre, informado e inequívoco
Direitos do Titular	Acesso aos dados	Acesso, retificação, exclusão, portabilidade, e direito ao esquecimento	Acesso, retificação, exclusão, portabilidade, anonimização, e direito ao esquecimento
Autoridade Reguladora	Departamento de Saúde e Serviços Humanos dos EUA (HHS)	Autoridades de Proteção de Dados de cada país-membro da UE	Autoridade Nacional de Proteção de Dados (ANPD)
Medidas de Segurança	Requer criptografia, controle de acesso e auditoria para ePHI	Exige segurança e minimização de dados, com recomendação de pseudonimização e anonimização	Exige segurança e minimização de dados, com recomendação de pseudonimização e anonimização
Penalidades por Violações	Multas variáveis conforme o tipo de violação e penalidades criminais em casos extremos	Até 4% do faturamento global anual ou 20 milhões de euros	Até 2% do faturamento ou 50 milhões de reais por infração
Ano de Implementação	1996	2018	2020

2.2.1 Health Insurance Portability and Accountability Act (HIPAA)

O **Health Insurance Portability and Accountability Act** (HIPAA), promulgado nos Estados Unidos em 1996, é uma legislação fundamental destinada a proteger a privacidade e a segurança das informações de saúde dos utentes, além de estabelecer padrões para a transmissão eletrônica de dados médicos. A HIPAA foi introduzida para responder a preocupações crescentes sobre o uso e o compartilhamento de informações de saúde em um cenário de transformação digital no setor de saúde [5].

Um dos aspectos centrais do HIPAA é o **Privacy Rule**, que estabelece diretrizes rígidas sobre como as informações de saúde protegidas (Protected Health Information - PHI) podem ser usadas e divulgadas. Esta regra garante que os dados pessoais de saúde dos utentes sejam acessíveis apenas para profissionais autorizados e utilizados exclusivamente para finalidades específicas, como tratamento, pagamento ou operações de saúde. Além disso, o Privacy Rule concede aos utentes o direito de acessar e corrigir suas informações de saúde, promovendo transparência e controle sobre os próprios dados [5].

Outro componente essencial é o **Security Rule**, que exige a implementação de medidas de segurança para proteger as informações de saúde em formato eletrônico (ePHI - electronic Protected Health Information). Esta regra estabelece requisitos técnicos e administrativos, incluindo a adoção de **controles de acesso, criptografia de dados e auditoria de acesso** para garantir rastreabilidade e que somente usuários autorizados possam acessar as informações sensíveis dos utentes. Além disso, o Security Rule obriga as organizações a implementar planos de contingência e políticas de recuperação de dados para proteger as informações em caso de falhas ou incidentes de segurança [5].

A **HIPAA** também introduz penalidades rigorosas para o descumprimento das diretrizes estabelecidas. As penalidades variam dependendo da gravidade e da natureza da violação e podem resultar em multas significativas, além de sanções adicionais em casos de negligência intencional [5]. Esse aspecto reforça o compromisso com a proteção de dados e incentiva as organizações a adotar medidas robustas de conformidade.

Em um contexto onde a digitalização da saúde avança rapidamente, o HIPAA desempenha um papel fundamental na proteção da privacidade e na segurança dos dados de saúde dos utentes. Suas diretrizes continuam a evoluir para acompanhar as novas tecnologias e práticas do setor, sendo um modelo de referência global para legislações e normas de proteção de dados de saúde.

2.2.2 General Data Protection Regulation (GDPR)

O **General Data Protection Regulation** (GDPR), implementado pela União Europeia em 2018, representa um marco na proteção dos dados pessoais, estabelecendo diretrizes rigorosas sobre a coleta, o armazenamento, o processamento e o compartilhamento de informações pessoais. Criado com o objetivo de garantir a privacidade e os direitos dos cidadãos da União Europeia, o GDPR não apenas harmoniza a legislação de proteção de dados em toda a União, mas também serve como referência para outros países ao redor do mundo.

Entre os pilares centrais do GDPR está o conceito de **consentimento informado**. Sob o regulamento, as organizações são obrigadas a obter um consentimento claro e explícito dos

indivíduos antes de coletar seus dados pessoais. O GDPR exige que o consentimento seja fornecido de forma transparente, informando ao indivíduo sobre a finalidade específica para a qual seus dados serão utilizados, além de permitir que ele revogue o consentimento a qualquer momento [6]. Esse princípio coloca o controle dos dados nas mãos dos indivíduos, promovendo uma relação mais transparente entre as organizações e os usuários.

Outro aspecto fundamental do GDPR é o **direito ao esquecimento**, que garante aos indivíduos a possibilidade de solicitar que seus dados sejam apagados quando não forem mais necessários para as finalidades originais ou caso o indivíduo retire seu consentimento [6]. Este direito fortalece a proteção da privacidade ao permitir que os cidadãos limitem o tempo de retenção de suas informações pessoais, reduzindo o risco de violações de dados ao longo do tempo.

O GDPR também introduz o **princípio da minimização de dados**, pelo qual as organizações devem coletar e processar apenas os dados estritamente necessários para atingir as finalidades específicas. Esse princípio visa reduzir a quantidade de dados sensíveis mantidos por organizações e minimizar o impacto de uma possível violação de segurança. Além disso, o GDPR recomenda o uso de técnicas como **pseudonimização** e **anonimização** para proteger informações pessoais, especialmente quando os dados precisam ser compartilhados ou analisados para fins de pesquisa [6].

Para reforçar a conformidade, o GDPR impõe sanções rigorosas para infrações, incluindo multas significativas que podem chegar a 4% do faturamento global anual da organização ou até 20 milhões de euros, o que for maior. Essas penalidades incentivam as organizações a priorizarem a segurança e a conformidade, integrando a proteção de dados pessoais como um elemento central de suas operações [6].

Assim, o GDPR estabelece um conjunto abrangente de diretrizes que não só protege os dados dos cidadãos da União Europeia, mas também orienta as melhores práticas de privacidade e segurança em nível global, promovendo uma abordagem ética e transparente na gestão de informações pessoais.

2.2.3 Lei Geral de Proteção de Dados Pessoais (LGPD)

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, instituída no Brasil pela Lei nº 13.709 de 2018, estabelece diretrizes sobre a coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais com o objetivo de proteger a privacidade dos cidadãos e promover a transparência nas operações que envolvem dados. Inspirada no **General Data Protection Regulation (GDPR)** da União Europeia, a LGPD harmoniza a legislação de proteção de dados no Brasil e cria um ambiente de segurança jurídica para indivíduos e organizações que operam no país [7].

Um dos princípios centrais da LGPD é o **consentimento do titular dos dados**. Sob a LGPD, o consentimento deve ser fornecido de forma livre, informada e inequívoca, após o titular dos dados ser devidamente informado sobre as finalidades específicas do tratamento. Esse princípio visa garantir que o controle sobre os dados pessoais permaneça nas mãos dos indivíduos, permitindo que eles tenham clareza sobre como e por que suas informações são utilizadas [7]. A LGPD também confere aos titulares dos dados uma série de direitos, incluindo o **direito de acesso** às suas informações, o **direito de correção** de dados incorretos, o **direito à anonimização**

e o **direito à exclusão** de dados pessoais quando estes não forem mais necessários para as finalidades informadas ou quando o titular revogar seu consentimento [7]. Esses direitos ampliam o controle do indivíduo sobre suas informações, promovendo uma gestão responsável e transparente dos dados pessoais.

Outro aspecto importante da LGPD é o **princípio da necessidade**, que orienta as organizações a coletarem e processarem apenas os dados estritamente essenciais para o alcance das finalidades específicas declaradas. Para proteger informações sensíveis, a LGPD recomenda o uso de técnicas de **pseudonimização** e **anonimização**, garantindo uma camada adicional de segurança, especialmente em processos de compartilhamento de dados ou análises estatísticas [7].

Para garantir a conformidade, a LGPD criou a **Autoridade Nacional de Proteção de Dados (ANPD)**, órgão responsável pela fiscalização e regulamentação das práticas de proteção de dados no Brasil. A ANPD possui a autoridade para aplicar sanções administrativas em casos de descumprimento, que podem variar desde advertências até multas de até 2% do faturamento da organização, com limite de 50 milhões de reais por infração [7]. Essas penalidades incentivam as empresas a adotarem medidas de conformidade e segurança, considerando a privacidade como um princípio essencial em suas operações.

Portanto, a LGPD não apenas protege os direitos dos cidadãos brasileiros, mas também estabelece um conjunto de normas que promovem práticas de gestão de dados responsáveis e transparentes no Brasil.

2.3 Interoperabilidade entre Sistemas de Saúde

A interoperabilidade entre sistemas de saúde é um dos maiores desafios enfrentados pelo setor, especialmente com o aumento da digitalização e da utilização de tecnologias móveis e **e-Health**. A capacidade de trocar dados entre diferentes plataformas e dispositivos médicos de forma eficiente e segura é fundamental para garantir a continuidade do cuidado e melhorar os resultados clínicos. Para que essa troca de informações seja possível, padrões como o **HL7 FHIR** e o **DICOM** desempenham um papel essencial, permitindo que dados de saúde sejam compartilhados entre diferentes sistemas de maneira padronizada e estruturada [1].

O **HL7 FHIR** (*Fast Healthcare Interoperability Resources*) é um padrão desenvolvido pela **Health Level Seven International (HL7)** que tem como objetivo facilitar a troca de dados clínicos entre diferentes sistemas de informação em saúde. Ele foi projetado para ser uma solução flexível e de fácil implementação, utilizando tecnologias modernas da web, como **APIs RESTful** e **JSON**, para garantir que os dados possam ser acessados e trocados de maneira rápida e eficiente. O FHIR permite a interoperabilidade de uma vasta gama de informações de saúde, desde registros eletrônicos de saúde (EHR) até dados de dispositivos móveis de saúde e monitoramento remoto. Ao adotar o FHIR, as organizações de saúde podem integrar dados de múltiplos sistemas e fornecer uma visão consolidada das informações do utente para médicos e outros profissionais de saúde.

Outro padrão crítico para a interoperabilidade em saúde é o **DICOM** (*Digital Imaging and Communications in Medicine*), que foi criado para garantir a troca padronizada de informa-

ções de imagens médicas entre dispositivos e sistemas. Utilizado em áreas como radiologia, cardiologia e oncologia, o DICOM permite que imagens médicas e informações associadas, como resultados de exames, sejam compartilhadas e acessadas de maneira interoperável entre diferentes dispositivos médicos e sistemas de informação. Isso é fundamental para o diagnóstico e tratamento, já que facilita o acesso a imagens médicas de alta qualidade por diferentes profissionais de saúde, independentemente do local onde foram capturadas.

A implementação de padrões como o **HL7 FHIR** e o **DICOM** não só facilita a troca de informações de saúde, como também promove uma maior eficiência operacional no setor. A interoperabilidade reduz a duplicação de testes e exames, melhora a precisão dos diagnósticos e permite que os profissionais de saúde tomem decisões mais informadas, com base em um panorama completo e atualizado dos dados do utente. Além disso, ao utilizar esses padrões, as organizações de saúde podem integrar novos dispositivos e tecnologias de forma mais rápida, garantindo que as inovações em saúde digital possam ser rapidamente incorporadas aos fluxos de trabalho clínicos [1].

Dessa forma, a adoção de padrões como o **HL7 FHIR** e o **DICOM** é essencial para promover a interoperabilidade entre sistemas de saúde, melhorar a qualidade do cuidado e otimizar a utilização de recursos no setor.

2.4 Diretrizes de Usabilidade e Acessibilidade

A acessibilidade em plataformas digitais é um aspecto essencial para garantir que todas as pessoas, independentemente de suas capacidades físicas ou cognitivas, possam utilizar aplicações web ou móveis de forma eficiente. Para garantir a inclusão e acessibilidade em ambientes digitais, foram desenvolvidas as **Web Content Accessibility Guidelines (WCAG)**, um conjunto de diretrizes voltadas para tornar o conteúdo web mais acessível a pessoas com **deficiências visuais, auditivas, motoras e cognitivas**. A adoção das **WCAG** é fundamental para assegurar que o maior número possível de usuários, incluindo aqueles com deficiências, possa interagir com a aplicação de maneira independente e eficiente [4].

As diretrizes **WCAG** estão organizadas em torno de quatro princípios principais: **perceptível, operável, compreensível e robusto**. Esses princípios visam garantir que a aplicação seja visualmente e auditivamente acessível, possa ser operada com diferentes tipos de dispositivos, como teclados ou assistentes de voz, e seja compreensível para uma ampla gama de usuários com diferentes níveis de conhecimento técnico ou habilidades cognitivas. Além disso, as diretrizes garantem que a aplicação seja robusta o suficiente para ser compatível com diferentes tecnologias assistivas.

Para pessoas com **deficiências visuais**, as diretrizes recomendam o uso de alternativas de texto para qualquer conteúdo não textual, como imagens, gráficos ou vídeos. Isso garante que usuários que utilizam leitores de tela possam compreender o conteúdo visual por meio de descrições textuais claras. Além disso, recomenda-se um contraste adequado de cores e a possibilidade de redimensionamento do texto, facilitando a leitura para pessoas com baixa visão.

Para aqueles com **deficiências auditivas**, as **WCAG** sugerem a implementação de legendas e

transcrições textuais para qualquer conteúdo de áudio ou vídeo, garantindo que as informações multimídia possam ser compreendidas por pessoas com perda auditiva. Da mesma forma, a navegação da aplicação deve ser totalmente operável por meio de teclados, o que é crucial para pessoas com **deficiências motoras**, que podem ter dificuldades no uso de dispositivos de apontamento, como o mouse [4].

Além disso, é importante considerar as necessidades de pessoas com **deficiências cognitivas**, garantindo que a interface do usuário seja intuitiva, com navegação clara e consistente. O uso de linguagem simples e a disponibilização de instruções claras podem facilitar a interação desses usuários com a aplicação.

A adoção das diretrizes **WCAG** não apenas garante a conformidade com os requisitos legais de acessibilidade digital em muitas regiões, como também promove uma melhor experiência de usuário para todas as pessoas. Ao considerar as necessidades de usuários com diferentes tipos de deficiência desde a fase de design, as aplicações se tornam mais inclusivas, eficientes e acessíveis para todos os usuários.

2.5 Aplicações Existentes no Mercado

Nos últimos anos, o mercado de **e-Health** tem experimentado um crescimento acelerado, com o surgimento de diversas aplicações destinadas a melhorar o acompanhamento de doentes, a gestão de informações de saúde e a comunicação entre utentes e profissionais de saúde. Essas soluções digitais oferecem funcionalidades variadas, desde o monitoramento remoto até o armazenamento seguro de dados médicos, sendo amplamente adotadas tanto por usuários finais quanto por instituições de saúde. Abaixo estão algumas das principais aplicações de **e-Health** disponíveis no mercado (comparação disponível na Tabela 2.2), sejam elas já consolidadas ou emergentes.

1. MyChart

MyChart é uma das soluções de **e-Health** mais amplamente utilizadas nos Estados Unidos. Desenvolvida pela Epic Systems, ela permite que os utentes acessem seus registros médicos de forma segura, façam o agendamento de consultas, visualizem resultados de exames e se comuniquem diretamente com seus médicos. Uma das características mais notáveis do **MyChart** é sua integração com registros eletrônicos de saúde (**EHR**), facilitando o compartilhamento de informações entre diversas instituições de saúde que utilizam o sistema da Epic. O MyChart está disponível em: <https://www.mychart.com>.

2. Teladoc Health

Teladoc Health é uma aplicação de telemedicina que oferece aos utentes consultas virtuais com profissionais de saúde em diversas especialidades. O serviço permite que os usuários recebam aconselhamento médico, diagnósticos e prescrições de maneira remota, eliminando a necessidade de visitas físicas em muitos casos. Teladoc é particularmente útil para o acompanhamento de doentes crônicos, fornecendo monitoramento contínuo e orientações médicas frequentes, o que foi amplamente adotado durante a pandemia de COVID-19. O Teladoc Health está disponível em: <https://www.teladochealth.com>.

3. HealthTap

HealthTap é uma aplicação emergente que utiliza inteligência artificial para conectar utentes a uma rede de médicos e especialistas. A aplicação oferece consultas virtuais, monitoramento remoto e recursos de autoatendimento, permitindo que os usuários façam perguntas e recebam respostas automatizadas baseadas em grandes bancos de dados clínicos. O HealthTap também possibilita que os utentes visualizem e armazenem seus dados de saúde em um ambiente seguro, utilizando padrões de privacidade como **HIPAA**. O HealthTap está disponível em: <https://www.healthtap.com>.

4. eMed

eMed é uma aplicação global de **e-Health** focada em perda de peso que oferece consultas virtuais com médicos e um sistema de IA que ajuda os utentes a diagnosticar sintomas comuns antes de consultar um profissional. A IA da Babylon faz perguntas ao usuário sobre seus sintomas e sugere possíveis condições médicas com base em algoritmos. Essa funcionalidade de triagem é seguida por uma consulta virtual com um médico, quando necessário. O Babylon também permite que os utentes acessem seus registros médicos e gerenciem consultas e prescrições de forma eficiente. O eMed está disponível em: <https://www.emed.com>.

5. Doximity

Doximity é uma plataforma de **e-Health** destinada a profissionais de saúde, permitindo que médicos e outros profissionais se conectem, compartilhem informações e se atualizem sobre as últimas pesquisas clínicas. A aplicação também oferece funcionalidades de comunicação segura entre médicos e seus utentes, além de permitir a realização de consultas remotas por vídeo. Com mais de um milhão de usuários registrados, o Doximity se destaca como uma das maiores redes profissionais de saúde no mundo. O Doximity está disponível em: <https://www.doximity.com>.

6. Ada Health

Ada Health é uma aplicação emergente que utiliza inteligência artificial para ajudar os utentes a monitorar sua saúde e identificar possíveis condições médicas com base nos sintomas relatados. A interface é simples e amigável, permitindo que os usuários insiram suas informações e recebam sugestões sobre possíveis diagnósticos, além de orientações sobre quando procurar ajuda médica. A aplicação também oferece a capacidade de armazenar e gerenciar registros de saúde pessoais.

Essas aplicações mostram a diversidade de soluções **e-Health** disponíveis no mercado, com abordagens que vão desde o monitoramento remoto e consultas virtuais até o uso de inteligência artificial para melhorar o atendimento e a gestão de dados médicos. Cada uma delas oferece funcionalidades valiosas que têm ajudado a transformar o modo como utentes e profissionais de saúde interagem, promovendo uma assistência mais eficiente e acessível. O Ada Health está disponível em: <https://www.ada.com>.

7. Telemonit SNS 24

O **Telemonit SNS 24** é uma solução de **telemonitorização** integrada ao **Serviço Nacional de Saúde (SNS) de Portugal**, voltada para o acompanhamento remoto de utentes com **doenças crônicas**. A plataforma permite que profissionais de saúde monitorem parâmetros vitais dos utentes em tempo real, reduzindo a necessidade de deslocamentos e promovendo um cuidado mais contínuo e preventivo.

Ferramentas para integração de informação médica

A aplicação possibilita que utentes registrem seus sinais clínicos, como **pressão arterial, glicemia, oxigenação do sangue e temperatura**, que são analisados automaticamente e enviados para as equipes médicas responsáveis. Caso sejam identificadas alterações significativas, alertas são gerados para intervenção rápida dos profissionais de saúde.

Além do monitoramento remoto, o **Telemonit SNS 24** promove a **educação em saúde**, fornecendo informações personalizadas sobre a condição do utente e incentivando hábitos saudáveis. A plataforma segue **padrões rigorosos de privacidade e segurança de dados**, garantindo conformidade com regulamentos como a **LGPD** e o **GDPR**.

Essa tecnologia tem se mostrado eficaz na **redução de internações hospitalares desnecessárias**, proporcionando maior qualidade de vida aos utentes e otimizando os recursos do sistema de saúde. O Telemonit SNS 24 está disponível em: <https://www.sns24.gov.pt/servico/app-telemonit-sns-24>.

Tabela 2.2: Tabela Comparativa de Aplicações de e-Health

Aplicação	Funcionalidades Principais	Destaques
MyChart	Acesso a registros médicos, agendamento de consultas, visualização de resultados	Integração com EHR de múltiplas instituições de saúde
Teladoc Health	Consultas virtuais com médicos, diagnósticos e prescrições remotas	Telemedicina amplamente utilizada, monitoramento de doentes crônicos
HealthTap	Consultas virtuais, IA para perguntas de saúde, armazenamento de dados de saúde	Uso de Inteligência Artificial para diagnósticos iniciais
eMed	Triagem por IA, consultas virtuais, gestão de registros médicos	Diagnósticos preliminares com IA seguidos por consultas médicas
Doximity	Rede profissional para médicos, consultas por vídeo, comunicação segura	Focada em profissionais de saúde, com mais de 1 milhão de usuários
Ada Health	IA para monitoramento de sintomas, gestão de registros pessoais de saúde	Interface amigável e personalização de diagnósticos com IA
Telemonit SNS 24	Monitoramento remoto de sinais vitais, envio de alertas, acompanhamento de utentes crônicos	Integrado ao SNS Portugal , suporte a LGPD e GDPR

2.6 Inteligência Artificial em e-Health

A utilização da **Inteligência Artificial (IA)** em **e-Health** tem revolucionado a maneira como os serviços de saúde são prestados e como as informações médicas são gerenciadas. A IA desempenha um papel crescente no diagnóstico, monitoramento, tratamento e gestão de dados clínicos, permitindo uma abordagem mais eficiente, precisa e personalizada no cuidado aos utentes. Aplicações de saúde baseadas em IA estão sendo usadas em diversas áreas, desde a triagem de sintomas até o suporte a decisões clínicas, fornecendo insights valiosos a partir de grandes volumes de dados [3].

Um dos principais usos da IA no setor de saúde é o **diagnóstico automatizado**. Ferramentas de

IA, como as utilizadas pela **Babylon Health** e **Ada Health**, são capazes de processar sintomas inseridos pelos utentes e gerar possíveis diagnósticos com base em algoritmos avançados. Essas ferramentas podem realizar uma triagem inicial, oferecendo sugestões aos usuários sobre o que pode estar causando seus sintomas antes que eles consultem um profissional de saúde. Esse tipo de automação melhora o tempo de resposta e reduz a carga de trabalho dos médicos, liberando-os para se concentrarem em casos mais complexos.

Outro uso relevante da IA está na **análise de dados médicos**. Grandes volumes de dados gerados por registros eletrônicos de saúde (**EHR**), dispositivos de monitoramento e exames laboratoriais podem ser analisados de forma eficiente por algoritmos de IA, que identificam padrões e tendências. Isso pode ajudar os profissionais de saúde a detectar alterações sutis nos dados de um utente, permitindo intervenções precoces em condições crônicas ou agudas. Além disso, a IA pode ser utilizada para prever desfechos clínicos, auxiliando na tomada de decisões sobre os melhores planos de tratamento.

Entretanto, a utilização da IA em **e-Health** também apresenta desafios importantes. Um dos principais problemas é a **transparência** dos algoritmos de IA, muitas vezes referida como o problema da "caixa-preta". Em muitos casos, os profissionais de saúde podem não entender completamente como um algoritmo chegou a determinada conclusão ou diagnóstico, o que pode gerar desconfiança e hesitação no uso dessas tecnologias [2]. Para que a IA seja amplamente adotada no setor de saúde, é essencial desenvolver sistemas explicáveis que permitam aos usuários compreenderem como os resultados são gerados.

Outro desafio é a **privacidade dos dados**. À medida que a IA processa grandes quantidades de informações pessoais de saúde, surge a necessidade de garantir que esses dados estejam protegidos conforme regulamentos como o **GDPR** e a **HIPAA**. A implementação de medidas robustas de segurança, como criptografia e pseudonimização, é essencial para garantir que os dados dos utentes estejam seguros e que os algoritmos de IA respeitem a privacidade dos usuários [2].

O futuro da IA em **e-Health** é promissor. A combinação de IA com a **Internet das Coisas (IoT)** tem o potencial de transformar a maneira como os utentes são monitorados, permitindo a coleta contínua de dados por meio de dispositivos vestíveis e sensores. Esses dados podem ser analisados em tempo real por sistemas de IA, fornecendo alertas e recomendações imediatas para profissionais de saúde e utentes. Além disso, avanços na IA, como **aprendizado profundo (deep learning)** e **redes neurais**, continuarão a melhorar a precisão dos diagnósticos e a capacidade de personalizar tratamentos com base nas características únicas de cada utente. Em resumo, a **Inteligência Artificial** já desempenha um papel fundamental em **e-Health**, com implicações significativas para a eficiência e a qualidade dos cuidados de saúde. No entanto, questões relacionadas à transparência, privacidade e confiabilidade precisam ser resolvidas para que essas tecnologias alcancem seu pleno potencial no setor.

Capítulo 3

Seleção de Metodologias e Tecnologias

Com o objetivo de atender ao escopo delineado nesta dissertação (descrito no Anexo A.1) e respeitar o cronograma estabelecido no Anexo A.2, foram selecionadas tecnologias e metodologias ágeis de gestão de projetos que possibilitam um desenvolvimento eficiente, incremental e adaptável. Esta seção descreve as ferramentas, frameworks e práticas utilizadas no processo de construção da aplicação, justificando cada escolha com base em critérios técnicos, funcionais e de viabilidade.

3.1 Frontend com Angular e Material

O **Angular** é uma plataforma de desenvolvimento de aplicações web baseada em TypeScript, desenvolvida e mantida pela *Google*. Ele oferece um conjunto abrangente de ferramentas para criar aplicações web dinâmicas e responsivas. Com sua arquitetura baseada em componentes, permite que os desenvolvedores criem interfaces de usuário modulares e reutilizáveis, garantindo um desenvolvimento eficiente e organizado [8].

Ele possui alguns elementos básicos (Figura 3.1) como: componentes, templates, diretivas, roteamento, módulos, serviços, injeção de dependências e ferramentas de infraestrutura que automatizam tarefas, como a de executar os testes unitários de uma aplicação. O Angular facilita a criação de **Single-Page Applications (SPA)** com um qualidade e produtividade [8].

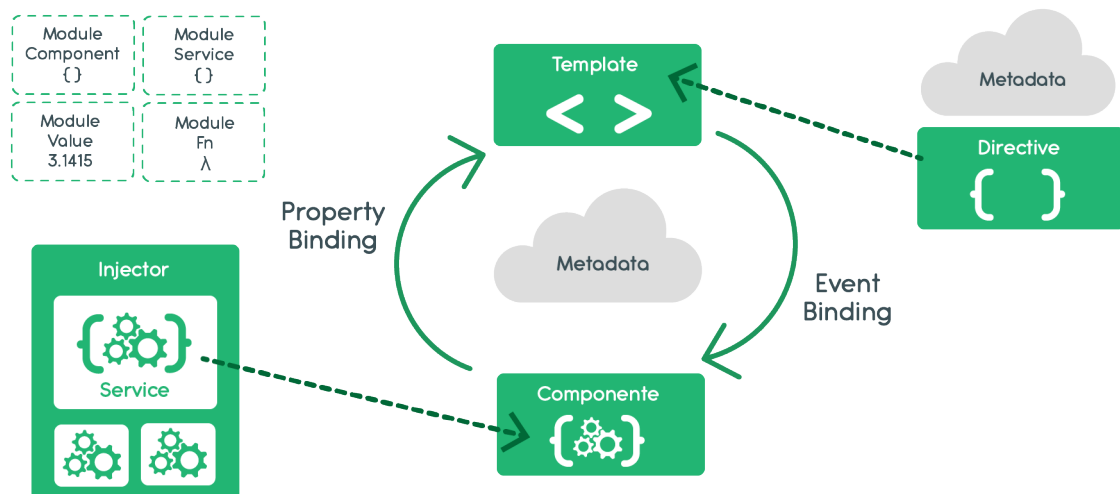


Figura 3.1: Arquitetura do Angular

O **Angular Material** é um conjunto de componentes de interface gráfica desenvolvido para integrar-se nativamente ao Angular. Baseado no sistema de design *Material Design*, ele fornece componentes visuais pré-construídos e consistentes que seguem diretrizes de usabilidade

e acessibilidade, otimizados para dispositivos móveis e desktop. Entre os componentes disponíveis, destacam-se botões, tabelas, formulários, ícones e elementos de navegação, todos projetados para proporcionar uma experiência de usuário uniforme e intuitiva [9].

A escolha do **Angular** e do **Material** para o desenvolvimento do frontend desta aplicação justifica-se pela sua capacidade de oferecer uma interface responsiva e funcional que pode ser acessada tanto por dispositivos móveis quanto por navegadores web. A arquitetura baseada em componentes do Angular facilita a criação de funcionalidades específicas, como o cadastro e o acompanhamento de informações de saúde pelos utentes, enquanto o Angular Material proporciona uma interface visual atrativa e consistente que segue os padrões modernos de design.

A aplicação permitirá que os **utentes** insiram e gerenciem informações de saúde, como medições, sintomas, alergias e intolerâncias, através de formulários intuitivos desenvolvidos com os componentes do Angular Material. Além disso, os utentes poderão acompanhar o estado de saúde por meio de gráficos e tabelas interativas que utilizam os componentes de visualização de dados do Angular. O uso dessas tecnologias garante que a interface seja acessível, eficiente e funcional em diferentes dispositivos e tamanhos de tela.

Portanto, o Angular e o Angular Material foram escolhidos não apenas por sua integração nativa e eficiência no desenvolvimento, mas também por sua capacidade de oferecer uma experiência de usuário intuitiva e familiar, essencial para o propósito da aplicação.

3.2 Firebase: Hosting, Authentication e Firestore

Firebase é uma plataforma baseada em nuvem projetada para o desenvolvimento de aplicativos web e móveis, ajudando a simplificar o processo de desenvolvimento [15].

O **Firebase** possibilita o desenvolvimento de aplicações móveis e web. Construído sobre os serviços subjacentes do **Google Cloud Platform (GCP)**, oferece um conjunto de ferramentas e serviços para facilitar o desenvolvimento, o gerenciamento e a escalabilidade de aplicativos. Dentre os recursos disponíveis, destacam-se o **Hosting**, **Authentication**, **Cloud Firestore** e **Storage**, que são amplamente utilizados para criar aplicações modernas e responsivas [15]. A Figura 3.2 ilustra o funcionamento de uma aplicação com acesso a recursos do Firebase.

3.2.1 Firebase Hosting

O **Firebase Hosting** é um serviço que permite o **hospedagem de aplicativos web** de forma rápida, segura e confiável. Ele suporta o deploy de arquivos estáticos, como HTML, CSS e JavaScript, bem como de aplicativos dinâmicos que utilizam frameworks modernos, como Angular, React e Vue.js. O Firebase Hosting inclui recursos como **certificados SSL automáticos**, suporte a **HTTP/2** e **CDN global**, garantindo alta performance e segurança para os usuários. Além disso, ele facilita o gerenciamento de diferentes versões do site, permitindo a realização de testes A/B e o rollback de versões [10].

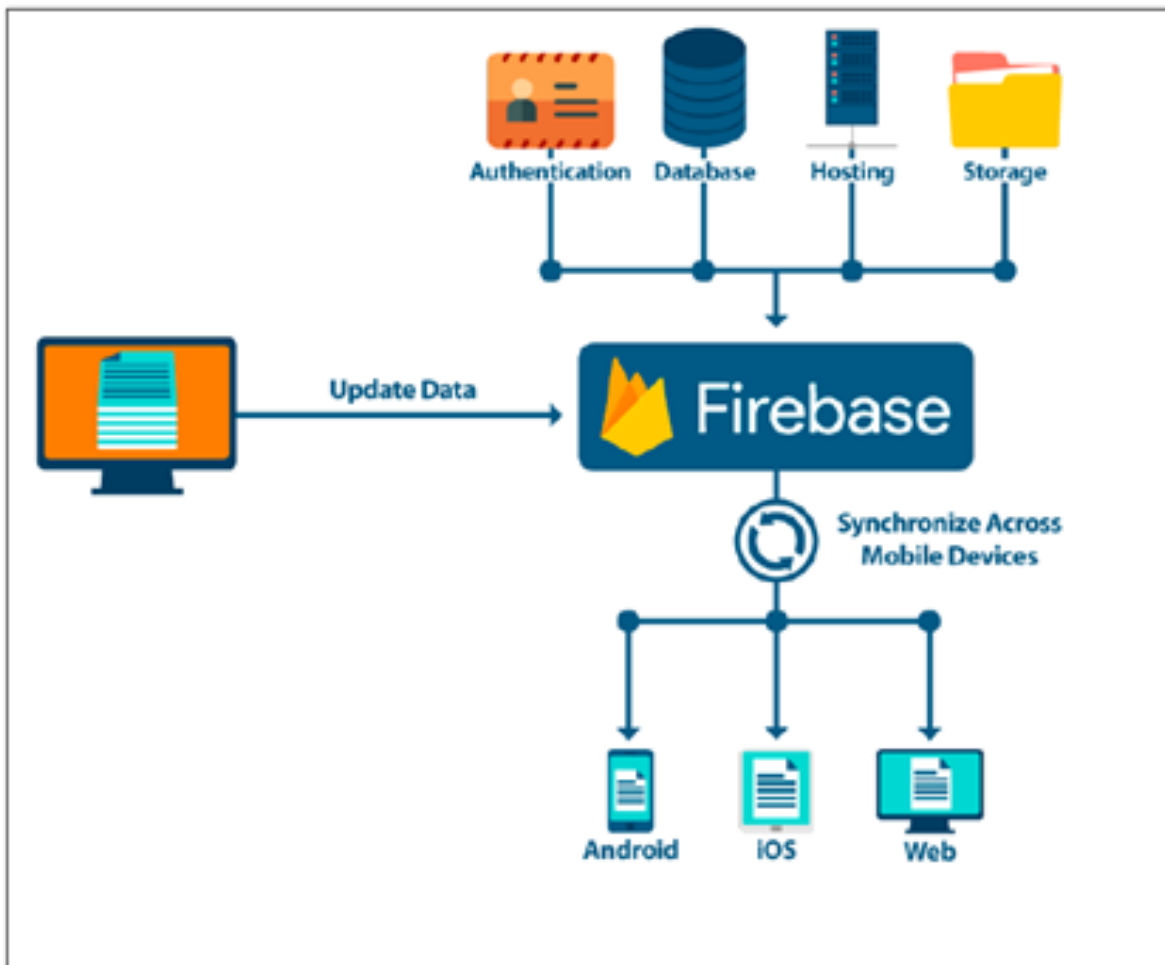


Figura 3.2: Funcionamento de Aplicação com Firebase

3.2.2 Firebase Authentication

O **Firebase Authentication** é uma solução que oferece métodos simples e seguros para autenticar usuários em aplicativos. Ele suporta diversos métodos de autenticação, como **email e senha**, **login social** (Google, Facebook, Twitter, entre outros) e **autenticação anônima**. Com uma integração direta com outros serviços do Firebase, como o Firestore e o Storage, o Authentication permite que desenvolvedores gerenciem identidades de usuários sem precisar construir um sistema de autenticação do zero. Além disso, ele inclui suporte para **autenticação multifator**, aumentando a segurança para os usuários [10].

3.2.3 Cloud Firestore

O **Cloud Firestore** é um banco de dados NoSQL em tempo real, otimizado para o armazenamento e sincronização de dados em aplicações móveis e web. Ele permite que os desenvolvedores armazenem, recuperem e sincronizem dados entre clientes e servidores de maneira eficiente. Com suporte para consultas avançadas, escalabilidade automática e integração com outros serviços do Firebase, como o Authentication e o Functions, o Firestore é ideal para aplicativos que exigem **sincronização em tempo real** ou **armazenamento offline**. Ele também oferece uma camada de segurança configurável baseada em regras, garantindo que apenas

usuários autorizados possam acessar os dados [10].

3.2.4 Conclusão

O Firebase, com seus serviços de Hosting, Authentication e Firestore, é uma solução poderosa para o desenvolvimento de aplicativos modernos, oferecendo ferramentas integradas que simplificam o processo de desenvolvimento e garantem alta escalabilidade e segurança. Sua flexibilidade permite que seja utilizado em uma ampla variedade de casos de uso, desde aplicativos simples até sistemas complexos de larga escala.

3.3 Análise Crítica das Tecnologias Adotadas

Nesta seção, realiza-se uma análise crítica das tecnologias escolhidas para o desenvolvimento do projeto, comparando-as com alternativas disponíveis no mercado e justificando as decisões tomadas.

3.3.1 Frontend com Angular e Material

O **Angular**, combinado com o **Angular Material**, foi selecionado como base para o desenvolvimento do frontend devido à sua arquitetura robusta e integração nativa. O Angular é uma plataforma de desenvolvimento baseada em **TypeScript**, que proporciona escalabilidade e organização no desenvolvimento de aplicações de médio a grande porte [8]. O Angular Material, por sua vez, oferece um conjunto de componentes visuais pré-construídos, seguindo as diretrizes de *Material Design*, o que facilita a criação de interfaces modernas, responsivas e acessíveis [9].

Alternativas Consideradas:

- **React (com Material-UI):** O React, mantido pelo Facebook, é outra opção amplamente utilizada para o desenvolvimento de aplicações web. Ele permite maior flexibilidade na escolha de bibliotecas de componentes, como o **Material-UI**, mas carece da integração nativa oferecida pelo Angular. Embora tenha uma curva de aprendizado mais suave, pode resultar em maior complexidade na configuração inicial.
- **Vue.js (com Vuetify):** O Vue.js é conhecido por sua simplicidade e leveza, sendo ideal para projetos de menor complexidade. Quando combinado com o **Vuetify**, oferece recursos semelhantes ao Angular Material, mas possui um ecossistema menor e menos orientado a aplicações empresariais de grande escala.

Justificativa: A escolha pelo **Angular** e **Angular Material** justifica-se pela sua arquitetura componentizada modular e pela integração nativa de ferramentas que simplificam o desenvolvimento de aplicações complexas, como é o caso deste sistema. Além disso, sua utilização de **TypeScript** promove maior segurança no código, enquanto o Angular Material garante uma interface consistente e acessível, essencial para utentes e profissionais de saúde.

3.3.2 Firebase

O **Firebase**, plataforma de **backend-as-a-service (BaaS)** desenvolvida pela Google, foi selecionado para o gerenciamento das funcionalidades de backend devido à sua simplicidade, integração e conjunto abrangente de ferramentas. Entre os serviços destacados estão: **Hosting** para hospedagem segura, **Authentication** para autenticação de usuários, **Firestore** para armazenamento de dados em tempo real e **Storage** para gerenciamento de arquivos [10].

Alternativas Consideradas:

- **AWS Amplify:** Plataforma da Amazon Web Services com funcionalidades similares ao Firebase, como autenticação, banco de dados e hospedagem. No entanto, possui uma curva de aprendizado mais complexa e custos mais elevados, especialmente para projetos de menor escala.
- **Azure App Services:** Serviço da Microsoft que permite o desenvolvimento, hospedagem e dimensionamento de aplicativos web e móveis. Ele oferece suporte a autenticação, integração com bancos de dados como Cosmos DB e serviços avançados como análises de dados.
 - **Pontos Fortes:** Integração nativa com o ecossistema Microsoft e suporte a linguagens populares como .NET, Node.js e Python.
 - **Limitações:** Modelo de precificação mais complexo e menos foco em pequenas equipes ou desenvolvedores individuais.
- **Supabase:** Uma alternativa *open-source* ao Firebase, baseada em **PostgreSQL**, que oferece suporte para autenticação e banco de dados em tempo real. Apesar de ser uma opção viável, ainda possui um ecossistema menos maduro e suporte técnico limitado.
- **Backend Tradicional (Node.js + Express):** Desenvolver um backend tradicional oferece maior flexibilidade e controle, permitindo personalizações avançadas. Contudo, exige maior esforço inicial para configuração, manutenção e segurança, o que aumenta o tempo de desenvolvimento.

Justificativa: O **Firebase** foi escolhido pela sua capacidade de acelerar o desenvolvimento, eliminando a necessidade de gerenciar servidores e infraestrutura. Sua integração nativa com serviços como **Firestore** e **Authentication** permite a criação de aplicações modernas e escaláveis, atendendo aos requisitos de segurança e desempenho do projeto. Além disso, sua abordagem *serverless* reduz significativamente os custos operacionais iniciais e a complexidade técnica, tornando-o uma escolha eficiente para este sistema.

3.3.3 Conclusão

Tanto o **Angular** com Angular Material quanto o **Firebase** foram escolhidos com base em sua capacidade de atender às demandas específicas deste projeto, equilibrando escalabilidade, simplicidade e eficiência. Enquanto o Angular e o Material destacam-se na construção de

interfaces modernas e acessíveis, o Firebase oferece um backend integrado e simplificado, eliminando a necessidade de infraestrutura cara e complexa.

Além disso, a escolha dessas ferramentas foi influenciada pela experiência prévia do autor com ambas as tecnologias. O uso consolidado do **Angular** e do **Firestore** em projetos anteriores permitiu uma curva de aprendizado mais rápida e a aplicação prática de boas práticas e padrões de desenvolvimento. Essa familiaridade também possibilita um maior domínio das funcionalidades oferecidas, maximizando a eficiência no desenvolvimento e reduzindo os riscos de implementação.

As alternativas consideradas, embora viáveis, apresentaram desvantagens em termos de integração, curva de aprendizado ou complexidade, o que reforça a adequação das tecnologias escolhidas para o desenvolvimento desta aplicação. Dessa forma, as ferramentas selecionadas proporcionam a base necessária para criar um sistema robusto, eficiente e alinhado às exigências do setor de saúde digital.

3.4 Uso de Progressive Web App (PWA)

A aplicação será desenvolvida como um **Progressive Web App (PWA)**, uma abordagem moderna que combina as melhores características de aplicações web e nativas. PWAs oferecem a experiência de um aplicativo nativo, como instalação em dispositivos, notificações e funcionamento offline, enquanto mantêm a acessibilidade e a simplicidade de uma aplicação web.

3.4.1 Características Principais de PWA

As principais características que justificam a escolha de PWA para o desenvolvimento incluem:

- **Instalação em Dispositivos:** PWAs podem ser instalados diretamente no dispositivo do usuário sem passar por lojas de aplicativos tradicionais, como Google Play ou App Store.
- **Desempenho Rápido:** PWAs utilizam técnicas de cache avançadas para carregar rapidamente e oferecer uma experiência fluida ao usuário.
- **Responsividade:** Desenvolvidos para serem acessíveis em qualquer dispositivo e tamanho de tela, PWAs garantem que a interface da aplicação seja adaptável a diferentes contextos de uso.
- **Atualizações Silenciosas:** Diferente de aplicativos tradicionais, PWAs podem ser atualizados automaticamente em segundo plano, garantindo que os usuários sempre utilizem a versão mais recente.

3.4.2 Vantagens de Utilizar PWA

A escolha por desenvolver a aplicação como PWA proporciona várias vantagens específicas para o contexto do projeto:

Ferramentas para integração de informação médica

- **Acessibilidade Ampliada:** Utentes podem acessar a aplicação diretamente pelo navegador ou instalá-la em seus dispositivos sem complicações.
- **Redução de Custos:** A abordagem PWA elimina a necessidade de desenvolver aplicativos separados para diferentes plataformas (iOS, Android, etc.), reduzindo custos e esforços de desenvolvimento.
- **Integração Simples:** Com a utilização do **Angular**, a configuração para transformar a aplicação em PWA é simplificada, com suporte nativo para *Service Workers* e caching.
- **Melhor Experiência do Usuário:** Notificações, funcionamento offline e desempenho rápido garantem uma experiência rica e satisfatória, fundamental para uma aplicação voltada à gestão de informações de saúde.

3.4.3 PWA no Contexto da Aplicação

No contexto do desenvolvimento da aplicação, o uso de PWA será estratégico para:

- Melhorar a acessibilidade da aplicação para utentes e profissionais de saúde, facilitando seu uso em dispositivos móveis e desktops.
- Proporcionar notificações sobre eventos importantes, como lembretes de medicação ou atualizações de informações de saúde.
- Garantir que a aplicação seja eficiente e responsiva, atendendo aos requisitos de desempenho e usabilidade definidos para o projeto.

A utilização do PWA alinha-se ao objetivo do projeto de criar uma solução acessível, eficiente e centrada no usuário, promovendo uma experiência consistente e satisfatória independentemente do dispositivo ou das condições de conectividade.

3.5 Versionamento de Código com Git e GitHub

O **Git** é um sistema de controle de versão distribuído amplamente utilizado no desenvolvimento de software para rastrear mudanças em arquivos e coordenar o trabalho entre múltiplos desenvolvedores. Com ele, é possível manter um histórico completo das alterações feitas no código, reverter mudanças indesejadas e facilitar a colaboração em projetos de qualquer escala. O **GitHub**, por sua vez, é uma plataforma baseada em nuvem que integra o Git a um conjunto de ferramentas para gerenciamento de repositórios, colaboração e automação, oferecendo um ambiente completo para equipes de desenvolvimento [13].

3.5.1 Funcionalidades do Git e GitHub

- **Controle de Versão Distribuído:** O Git permite que cada desenvolvedor tenha uma cópia completa do repositório em seu dispositivo, o que garante que o trabalho continue mesmo sem acesso à internet. Com o GitHub, os repositórios podem ser armazenados de forma centralizada na nuvem, permitindo que equipes compartilhem suas mudanças de maneira eficiente [13].

- **Branches e Colaboração:** O sistema de **branches** do Git possibilita que os desenvolvedores criem ramificações independentes do código principal, permitindo o desenvolvimento de novas funcionalidades sem interferir no trabalho de outros. No GitHub, esses branches podem ser integrados ao fluxo de trabalho colaborativo por meio de **pull requests**, onde as mudanças são revisadas antes de serem mescladas ao código principal [13].
- **Histórico e Rastreabilidade:** O Git mantém um histórico completo de todas as alterações feitas no código, incluindo autor, data e descrição das mudanças. Essa rastreabilidade é essencial para entender o contexto de alterações e reverter mudanças, se necessário. O GitHub complementa isso com uma interface visual para navegar no histórico do repositório [13].
- **Integrações e Automação:** O GitHub oferece suporte a ferramentas de automação, como **GitHub Actions**, que permitem configurar fluxos de trabalho automatizados para tarefas como testes, builds e deploys. Além disso, ele se integra a uma ampla gama de ferramentas externas, como IDEs e serviços de CI/CD, para otimizar o processo de desenvolvimento [13].

3.5.2 Importância para o Projeto

A utilização do Git e do GitHub neste projeto é fundamental para garantir a organização, o rastreamento e a colaboração eficaz no desenvolvimento da aplicação. Com o Git, os desenvolvedores podem trabalhar simultaneamente em diferentes funcionalidades sem risco de sobrescrever o trabalho uns dos outros. Além disso, a integração com o GitHub oferece uma plataforma centralizada para armazenar o código, revisar mudanças e gerenciar releases. No contexto de equipes distribuídas, o GitHub é especialmente útil, pois permite que os desenvolvedores colaborem remotamente e mantenham um controle rigoroso sobre o progresso do projeto. Recursos como **issues** e **project boards** ajudam a organizar tarefas e acompanhar o status do desenvolvimento, promovendo uma maior transparência e eficiência no gerenciamento do projeto.

Por fim, a combinação do Git com o GitHub garante que o histórico do código seja preservado e que mudanças possam ser auditadas, revertidas ou aprimoradas com facilidade, contribuindo para a qualidade e a sustentabilidade do projeto a longo prazo.

3.6 Boas Práticas em DevOps

No contexto de DevOps, as práticas de **Integração Contínua (Continuous Integration - CI)** e **Entrega Contínua (Continuous Delivery - CD)** são fundamentais para garantir a agilidade, a qualidade e a eficiência no desenvolvimento de software. Essas práticas promovem a automação de processos críticos, como testes e deploys, reduzindo o risco de erros e acelerando o ciclo de desenvolvimento. Neste projeto, a utilização de **GitHub Actions** para implementar CI/CD é essencial para alcançar esses objetivos [14].

3.6.1 Integração Contínua (CI)

A **Integração Contínua (CI)** é uma prática que envolve a integração frequente do código desenvolvido por diferentes membros da equipe em um repositório central. Cada integração é automaticamente validada por um conjunto de testes automatizados, garantindo que o código seja funcional e esteja em conformidade com os padrões definidos. No GitHub, a CI pode ser configurada usando o **GitHub Actions**, que permite executar pipelines de teste sempre que um novo código é enviado ao repositório [14].

No contexto deste projeto, a CI garante que todas as alterações sejam testadas antes de serem mescladas à base de código principal. Isso reduz o risco de introdução de bugs e facilita a colaboração entre os membros da equipe, promovendo um fluxo de trabalho mais eficiente e confiável.

3.6.2 Entrega Contínua (CD)

A **Entrega Contínua (CD)** é uma extensão da CI que automatiza a entrega de código para ambientes de produção ou pré-produção. Após a validação do código por meio da CI, o CD cuida de tarefas como a criação de builds e o deploy de novas versões da aplicação. Com o **GitHub Actions**, é possível configurar pipelines de deploy que automatizam essas etapas, garantindo que as atualizações cheguem rapidamente aos usuários [14].

No projeto, a CD é crucial para agilizar a entrega de novas funcionalidades e correções, reduzindo o tempo de feedback e aumentando a satisfação dos usuários.

3.6.3 GitHub Actions

O **GitHub Actions** é uma plataforma de automação integrada ao GitHub, que permite configurar e executar fluxos de trabalho diretamente nos repositórios. Ele suporta a criação de pipelines personalizáveis, que podem incluir etapas de build, teste e deploy, com suporte a diferentes linguagens e ambientes. Além disso, o GitHub Actions oferece uma ampla biblioteca de **ações pré-configuradas** e a capacidade de criar ações personalizadas, tornando-o uma ferramenta flexível e poderosa [14].

3.6.3.1 Funcionalidades do GitHub Actions

- **Triggers Automatizados:** Permite que pipelines sejam acionados automaticamente com base em eventos, como push, pull request ou lançamento de uma nova tag no repositório [14].
- **Suporte Multiplataforma:** Oferece suporte para executar fluxos de trabalho em ambientes Linux, macOS e Windows, permitindo a construção e o teste de aplicações em múltiplos sistemas [14].
- **Integração com CI/CD:** Facilita a configuração de pipelines completos de CI/CD, incluindo testes, builds e deploys automatizados, diretamente a partir do repositório [14].
- **Ações Reutilizáveis:** Inclui uma vasta biblioteca de ações pré-definidas e a capacidade de criar e compartilhar ações personalizadas entre diferentes repositórios [14].

3.6.4 Importância para o Projeto

A implementação de **CI/CD** com **GitHub Actions** neste projeto garante que o desenvolvimento ocorra de forma ágil e segura. Com pipelines automatizados, é possível identificar e corrigir problemas rapidamente, liberar novas funcionalidades com maior frequência e manter um alto nível de qualidade no código. Além disso, a integração nativa com o repositório GitHub centraliza todo o fluxo de trabalho em uma única plataforma, simplificando a colaboração e o gerenciamento do projeto.

Por fim, o uso de GitHub Actions permite escalar o desenvolvimento de forma eficiente, proporcionando uma base sólida para a evolução contínua da aplicação.

3.7 Metodologias Utilizadas para Gerir Tarefas

3.7.1 Metodologias Ágeis e sua Importância

As **Metodologias Ágeis** são abordagens de gerenciamento de projetos que enfatizam a colaboração, a flexibilidade, a entrega incremental de valor e a adaptação contínua às mudanças. Criadas originalmente para o desenvolvimento de software, essas metodologias se baseiam nos princípios do **Manifesto Ágil**, que prioriza indivíduos e interações, software funcional, colaboração com o cliente e resposta às mudanças em detrimento de processos rígidos e documentação extensiva [11].

3.7.1.1 Benefícios das Metodologias Ágeis em Projetos de Desenvolvimento de Aplicações

- **Entrega Incremental de Valor:** Em vez de esperar pela conclusão de todo o projeto, as metodologias ágeis permitem a entrega de funcionalidades em pequenos incrementos, conhecidos como **sprints**. Isso garante que os usuários possam começar a usar e avaliar o produto em um estágio inicial, fornecendo feedback valioso para as próximas iterações [11].
- **Colaboração e Comunicação:** As metodologias ágeis promovem uma comunicação frequente e eficiente entre todos os membros da equipe e os stakeholders. Ferramentas como o **Scrum** utilizam cerimônias como **daily stand-ups** e **reviews** para manter o alinhamento da equipe e garantir que todos estejam cientes do progresso do projeto [11].
- **Flexibilidade e Adaptação:** A capacidade de se adaptar a mudanças de requisitos é um dos pilares do Ágil. Em projetos como este, onde o feedback dos utentes e dos profissionais de saúde pode gerar novos requisitos ou mudanças nas funcionalidades, a metodologia ágil garante que essas alterações possam ser incorporadas sem grandes impactos no cronograma geral [11].
- **Foco na Qualidade:** Ao dividir o trabalho em pequenos ciclos, as equipes podem focar na qualidade de cada entrega, adotando práticas como **testes automatizados** e **integração contínua**. Isso resulta em um produto mais robusto e alinhado às expectativas dos usuários [11].

- **Engajamento do Cliente:** O Ágil promove a colaboração direta com os clientes durante todo o projeto. Isso garante que o produto final reflita as necessidades reais dos usuários, especialmente em um projeto como este, onde a experiência do utente é fundamental [11].

3.7.1.2 Importância para Projetos de Desenvolvimento de Aplicações em Saúde

No contexto de desenvolvimento de aplicações voltadas para saúde, as metodologias ágeis são particularmente valiosas. Esses projetos geralmente envolvem múltiplos stakeholders, como utentes, profissionais de saúde e desenvolvedores, cada um com suas próprias necessidades e prioridades. A abordagem ágil permite que essas diferentes perspectivas sejam integradas de forma eficiente durante o ciclo de desenvolvimento, garantindo que o produto final seja útil, seguro e funcional.

Além disso, projetos em saúde frequentemente requerem conformidade com regulamentações e padrões, como **HIPAA**, **GDPR** ou **LGPD**, o que pode demandar mudanças de última hora. As metodologias ágeis permitem que essas adaptações sejam feitas sem comprometer o progresso geral do projeto, mantendo a flexibilidade e o foco na entrega de valor.

Portanto, a adoção de metodologias ágeis não apenas melhora a eficiência e a qualidade do desenvolvimento, mas também assegura que o produto final atenda às expectativas e necessidades de seus usuários, sendo uma abordagem essencial para o sucesso de projetos como o descrito.

3.7.2 Trello e Quadro Kanban

O **Trello** é uma ferramenta de gerenciamento de projetos baseada em nuvem que utiliza o conceito de **quadro Kanban** para organizar e monitorar tarefas. Desenvolvido pela Atlassian, o Trello oferece uma interface visual simples e intuitiva, que permite que equipes e indivíduos acompanhem o progresso de atividades de forma colaborativa. Com o uso de quadros, listas e cartões, o Trello facilita a organização de fluxos de trabalho em diferentes projetos, garantindo maior clareza e produtividade [12].

3.7.2.1 Quadro Kanban

O **Kanban** é uma metodologia visual para gerenciamento de tarefas, baseada na ideia de limitar o trabalho em progresso e promover o fluxo contínuo de atividades. No Trello, o quadro Kanban é representado por **listas**, que podem ser configuradas para refletir diferentes estágios de um processo, como "A Fazer", "Em Progresso" e "Concluído". Cada tarefa é representada por um **cartão**, que pode ser movido entre as listas à medida que o trabalho avança [12].

A utilização do Kanban no Trello permite que as equipes tenham uma visão clara do estado atual de cada tarefa, identifiquem gargalos no fluxo de trabalho e priorizem atividades de maneira eficiente. Além disso, o sistema incentiva a transparência e a colaboração, pois todos os membros da equipe podem visualizar as tarefas em andamento e seu progresso (Figura 3.3).

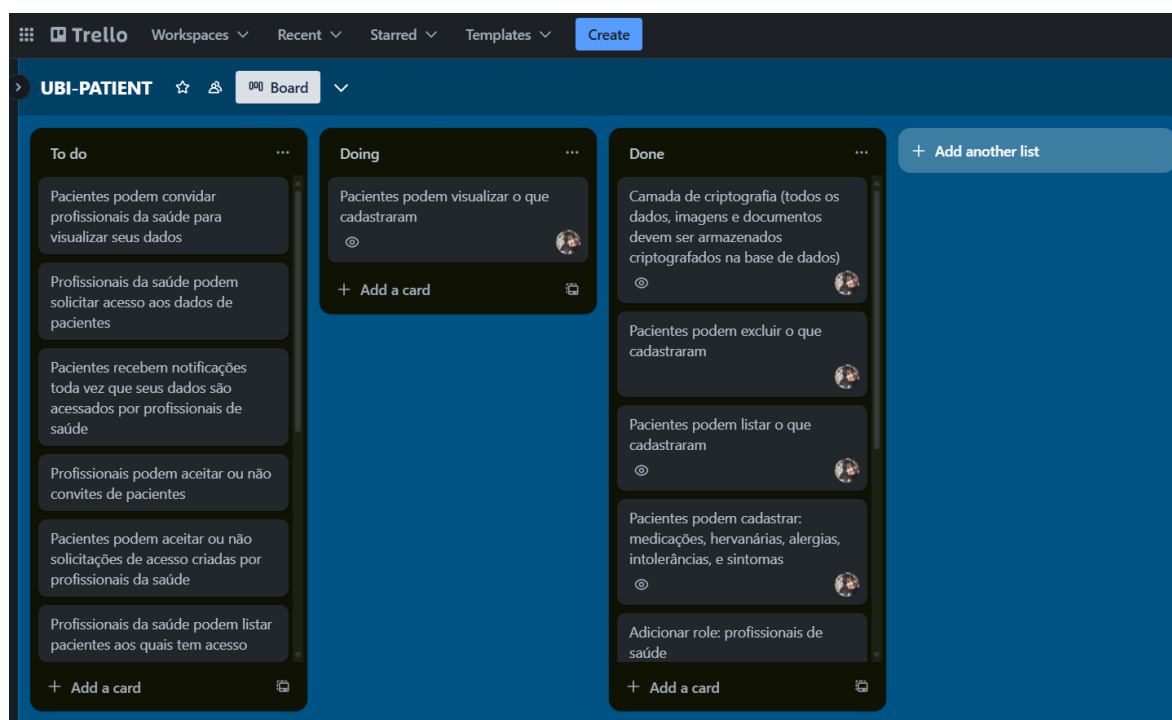


Figura 3.3: Quadro Kanban no Trello

3.7.2.2 Funcionalidades do Trello

O Trello oferece diversas funcionalidades que tornam o gerenciamento de projetos mais eficiente, incluindo:

- **Cartões:** Cada cartão representa uma tarefa e pode incluir detalhes como descrições, prazos, anexos, checklists e comentários. Esses elementos permitem que as equipes documentem todas as informações relevantes diretamente nos cartões, facilitando o acompanhamento e a comunicação [12].
- **Etiquetas e Filtros:** Os cartões podem ser categorizados com etiquetas coloridas, que ajudam a priorizar tarefas ou indicar tipos específicos de trabalho. Além disso, o Trello permite filtrar os cartões com base em etiquetas ou outros critérios, tornando mais fácil localizar informações específicas [12].
- **Automatização com Butler:** O Trello inclui o recurso **Butler**, que permite a criação de regras de automação para tarefas repetitivas. Com o Butler, é possível configurar ações automáticas, como mover cartões entre listas ou enviar notificações com base em gatilhos predefinidos, otimizando o fluxo de trabalho [12].
- **Integrações:** O Trello integra-se com diversas ferramentas populares, como Google Drive, Slack e Jira, permitindo que as equipes trabalhem de maneira conectada e centralizem suas atividades em um único lugar [12].
- **Relatórios e Visões Avançadas:** Além do quadro Kanban tradicional, o Trello oferece visões adicionais, como o **calendário**, para acompanhar prazos, e o **timeline**, que permite visualizar a distribuição de tarefas ao longo do tempo [12].

3.7.2.3 Importância para o Projeto

A utilização do Trello e do quadro Kanban é especialmente útil em projetos que requerem alta organização e colaboração, como o desenvolvimento de aplicativos descrito neste trabalho. A abordagem visual e flexível do Trello permite que todos os membros da equipe acompanhem o progresso das tarefas, identifiquem prioridades e ajustem o planejamento conforme necessário. Além disso, a transparência promovida pela ferramenta garante que todas as partes interessadas estejam alinhadas quanto aos objetivos e às etapas do projeto.

Com a combinação de simplicidade e recursos avançados, o Trello e o quadro Kanban oferecem uma solução poderosa para melhorar a produtividade e a eficiência em projetos colaborativos, sendo uma escolha ideal para equipes que buscam gerenciar seus fluxos de trabalho de maneira ágil e eficaz.

Capítulo 4

Padrões e Diretrizes de Segurança

4.1 Privacidade dos Dados

A privacidade dos dados é um aspecto central no desenvolvimento da aplicação, especialmente devido à sensibilidade das informações de saúde gerenciadas. Para garantir conformidade com as regulamentações **HIPAA**, **GDPR** e **LGPD**, a aplicação foi projetada com medidas robustas de segurança e políticas claras de privacidade.

4.1.1 Conformidade com Regulamentações

- **HIPAA**: A aplicação atenderá aos requisitos da **Health Insurance Portability and Accountability Act (HIPAA)** para proteger as informações de saúde protegidas (PHI - Protected Health Information). Isso inclui o uso de criptografia, controle de acesso e monitoramento de atividades para evitar acessos não autorizados.
- **GDPR**: Para estar em conformidade com o **General Data Protection Regulation (GDPR)**, a aplicação garantirá o consentimento informado dos utentes para o tratamento de dados, implementará o **direito ao esquecimento**, e permitirá o acesso e a portabilidade dos dados pelos utentes.
- **LGPD**: Seguindo as diretrizes da **Lei Geral de Proteção de Dados (LGPD)**, a aplicação garantirá a coleta e o processamento apenas dos dados necessários, implementará a anonimização e permitirá o acesso e a exclusão de informações conforme solicitado pelos utentes.

4.1.2 Medidas de Segurança

4.1.2.1 Criptografia

A aplicação foi projetada com um forte foco em segurança, utilizando **criptografia de ponta a ponta** para proteger os dados em **repouso** e em **trânsito**. Para os dados armazenados (Figura 4.1), será adotado o padrão de criptografia **AES-256**, um dos mais seguros atualmente disponíveis, amplamente utilizado em sistemas financeiros e governamentais. Já para os dados transmitidos entre o cliente e o servidor, será implementado o protocolo **TLS 1.3**, que garante segurança durante a comunicação e evita ataques de interceptação.

Essa abordagem robusta assegura que as informações sensíveis dos utentes, como medicações, sintomas e outros dados pessoais, permaneçam protegidas contra acessos não autorizados, mesmo em cenários de ataques avançados. Além disso, a implementação dessas técnicas está alinhada às diretrizes de segurança de normas como **HIPAA**, **GDPR** e **LGPD**, atendendo aos requisitos legais e regulamentares de privacidade [2].

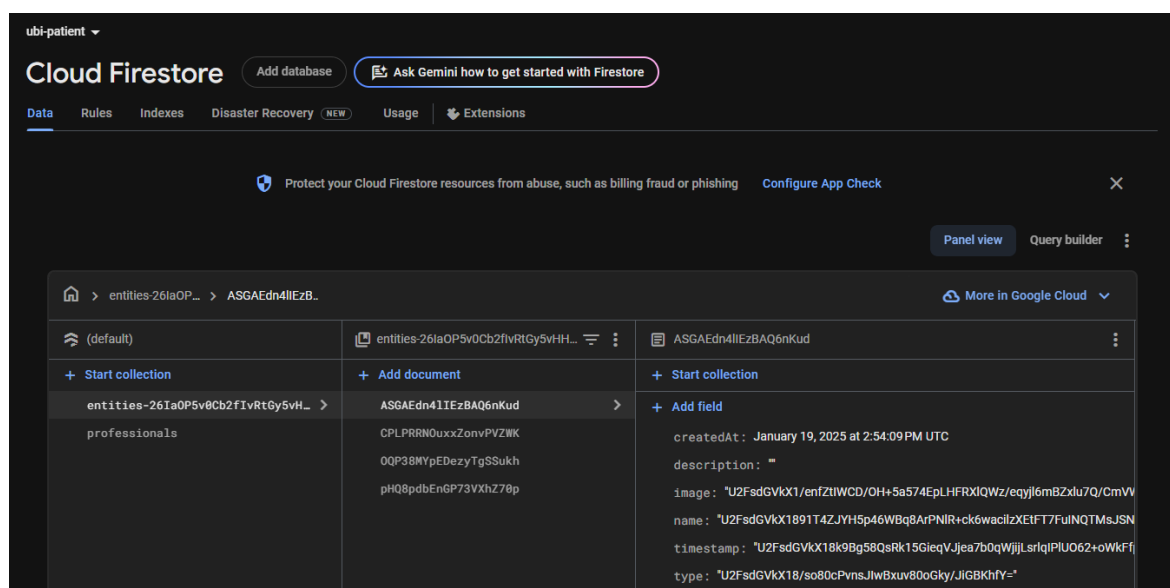


Figura 4.1: Informações Criptografadas no Firestore

4.1.2.2 AES-256

O **AES-256** (*Advanced Encryption Standard - 256 bits*) é um algoritmo de criptografia simétrica reconhecido globalmente como um dos métodos mais seguros para proteger dados confidenciais. Ele foi estabelecido como padrão pelo **National Institute of Standards and Technology (NIST)** em 2001 e é amplamente utilizado em aplicações que exigem alto nível de segurança, como sistemas bancários, governamentais e de saúde.

O **AES-256** funciona utilizando uma chave de 256 bits para criptografar e descriptografar os dados, oferecendo proteção contra ataques de força bruta devido ao vasto espaço de chaves possíveis. Sua principal vantagem é a combinação de alta segurança com eficiência de desempenho, tornando-o adequado tanto para dispositivos móveis quanto para servidores de alto desempenho.

As principais características do **AES-256** incluem:

- **Segurança Avançada:** Com 2^{256} combinações possíveis de chave, é praticamente impossível quebrar a criptografia utilizando métodos tradicionais.
- **Eficiência:** Projetado para ser eficiente em hardware e software, o AES-256 oferece alto desempenho mesmo em sistemas de baixa potência, como dispositivos móveis.
- **Flexibilidade:** Pode ser implementado em diversos cenários, incluindo bancos de dados, armazenamento em nuvem e comunicações seguras (Figura 4.2).

A utilização do **AES-256** no armazenamento de dados em trânsito e em repouso garantirá que, mesmo em caso de comprometimento físico do dispositivo ou servidor, as informações permaneçam inacessíveis sem a chave de descriptografia. Essa abordagem reforça a segurança e protege os dados dos utentes contra uma ampla gama de ameaças, alinhando-se às melhores práticas globais de proteção de dados.

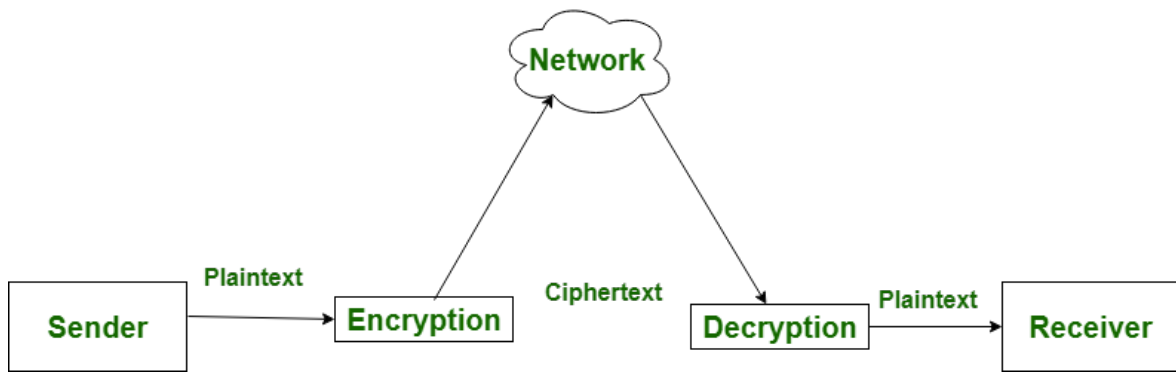


Figura 4.2: Criptografia AES

4.1.2.3 Logs de Auditoria

Serão implementados **logs de auditoria** detalhados para registrar todas as interações com os dados. Cada acesso ou modificação será documentado com as seguintes informações:

- Identidade do usuário responsável pela ação;
- Data e horário do evento;
- Tipo de operação realizada (leitura, atualização ou exclusão);
- Dados ou áreas específicas acessadas ou alteradas.

Esses logs serão armazenados de forma segura e somente acessíveis por administradores autorizados, garantindo a rastreabilidade e a detecção de acessos indevidos.

4.1.2.4 Controle de Acesso

A aplicação implementará **controle de acesso baseado em papéis (RBAC - Role-Based Access Control)**, garantindo que cada usuário tenha acesso apenas às informações relevantes para seu papel. Utentes poderão acessar e gerenciar apenas seus próprios dados, enquanto profissionais de saúde terão acesso limitado, dependendo das permissões concedidas pelos utentes.

4.1.2.5 Pseudonimização e Anonimização

Para mitigar riscos em caso de violação de dados, a aplicação empregará **pseudonimização** e **anonimização** sempre que possível. Dados sensíveis serão processados de maneira que identidades não possam ser vinculadas diretamente a indivíduos, exceto com chaves de descryptografia específicas.

4.1.3 Importância das Medidas de Privacidade

Ao implementar essas medidas de segurança e privacidade, a aplicação não apenas atende às exigências legais, mas também constrói confiança entre os utentes e os profissionais de saúde. O uso de criptografia, logs de auditoria e controle de acesso garante que os dados sejam protegidos contra ameaças internas e externas, promovendo um ambiente seguro e confiável para a gestão de informações sensíveis.

4.2 Gestão de Segurança da Informação em Saúde

A gestão de segurança da informação é um aspecto crítico no setor de saúde, especialmente devido à sensibilidade dos dados médicos e à crescente digitalização dos sistemas de saúde. Neste contexto, a **ISO 27799** é uma norma internacional que complementa a **ISO 27001**, mas com um foco específico na proteção de dados de saúde. Juntas, essas normas oferecem um framework abrangente para gerenciar e proteger informações sensíveis, com diretrizes claras sobre a implementação de medidas de segurança adequadas.

4.2.1 ISO 27001: Base para a Gestão da Segurança da Informação

A **ISO 27001** é uma norma internacional amplamente reconhecida que especifica os requisitos para a implementação de um **Sistema de Gestão de Segurança da Informação (SGSI)**. Ela fornece um conjunto de controles de segurança e práticas recomendadas para proteger informações contra acessos não autorizados, garantir a integridade dos dados e assegurar sua disponibilidade. Embora abrangente, a ISO 27001 não trata de maneira específica as particularidades dos dados médicos, o que é abordado pela ISO 27799.

4.2.2 ISO 27799: Foco em Dados de Saúde

A **ISO 27799** foi desenvolvida para complementar a ISO 27001, fornecendo diretrizes específicas para a proteção de **informações de saúde pessoal (PHI - Personal Health Information)**. Essa norma aplica os princípios gerais de segurança da ISO 27001, mas os adapta ao contexto particular da saúde, considerando as características únicas desse setor. A ISO 27799 orienta as organizações a proteger informações sensíveis relacionadas a diagnósticos, tratamentos, dados clínicos e registros médicos eletrônicos.

4.2.2.1 Principais Recomendações da ISO 27799

- **Identificação e Classificação de Dados de Saúde:** A norma enfatiza a necessidade de identificar e classificar adequadamente as informações de saúde, considerando seu nível de sensibilidade e o impacto potencial de violações de segurança.
- **Medidas de Controle Específicas para Dados Médicos:** Propõe controles adaptados ao ambiente de saúde, como autenticação robusta para profissionais, restrição de acesso a dados confidenciais e auditorias regulares para monitorar a conformidade.
- **Proteção contra Ameaças Internas e Externas:** Recomenda a implementação de criptografia, firewalls, e sistemas de detecção de intrusões para proteger dados contra ameaças externas, bem como políticas de conscientização para prevenir violações internas.
- **Gestão de Incidentes de Segurança em Saúde:** Define processos específicos para identificar, reportar e mitigar incidentes relacionados a dados de saúde, incluindo o planejamento de respostas rápidas para minimizar impactos em pacientes.

- **Conformidade com Regulamentações de Saúde:** Integra requisitos de conformidade com regulamentações locais e internacionais, como **HIPAA**, **GDPR** e **LGPD**, garantindo alinhamento legal.

4.2.3 Complementaridade entre ISO 27799 e ISO 27001

Enquanto a **ISO 27001** fornece um framework genérico para a gestão de segurança da informação em qualquer setor, a **ISO 27799** adapta essas diretrizes às necessidades específicas de organizações de saúde. A combinação dessas normas garante que as práticas de segurança sejam implementadas de maneira robusta e que os dados de saúde sejam protegidos contra ameaças variadas, atendendo às expectativas dos pacientes e às exigências legais.

4.2.4 Importância da Implementação

A implementação conjunta da ISO 27001 e ISO 27799 permite que as organizações de saúde adotem uma abordagem sistemática para proteger informações de saúde sensíveis. Isso não apenas reduz o risco de violações de dados, mas também melhora a confiança dos pacientes, assegura a conformidade com regulamentações e promove a eficiência operacional. Com a digitalização crescente no setor, essas normas tornam-se indispensáveis para garantir a segurança e a privacidade dos dados médicos.

4.3 Interoperabilidade com Padrões de Saúde

A interoperabilidade é um aspecto essencial para garantir a integração eficaz entre sistemas de saúde, promovendo a troca de informações de forma segura e padronizada. No contexto deste projeto, a utilização do padrão **HL7 FHIR (Fast Healthcare Interoperability Resources)** será fundamental para permitir a comunicação entre a aplicação e sistemas hospitalares, farmácias e outros provedores de serviços de saúde.

4.3.1 HL7 FHIR: Padrão para Interoperabilidade

O **HL7 FHIR** é um padrão internacional desenvolvido pela **Health Level Seven International (HL7)**, projetado para facilitar a troca de dados de saúde entre sistemas diferentes. Ele combina as melhores práticas de interoperabilidade com tecnologias modernas, como **APIs RESTful**, **JSON** e **XML**, tornando sua implementação mais flexível e eficiente em comparação com padrões anteriores, como: HL7 V3 e CDA (Clinical Document Architecture).

O HL7 FHIR estrutura os dados de saúde em recursos (resources) modulares, que representam entidades como pacientes, medicamentos, consultas, exames e prescrições. Esses recursos podem ser compartilhados entre sistemas, garantindo que as informações sejam interpretadas de maneira consistente, independentemente da plataforma utilizada.

4.3.2 Benefícios da Interoperabilidade com HL7 FHIR

- **Continuidade do Cuidado:** Permite que informações relevantes acompanhem o utente em diferentes provedores de saúde, garantindo uma visão integrada de seu estado clínico.

- **Redução de Redundâncias:** Elimina a necessidade de repetir exames ou registrar dados manualmente em múltiplos sistemas, economizando tempo e recursos.
- **Melhoria na Qualidade dos Dados:** Garante que as informações trocadas entre sistemas sejam consistentes, reduzindo erros relacionados a interpretações incorretas ou falta de dados.
- **Adoção de Tecnologias Modernas:** O uso de APIs RESTful e formatos de dados como JSON melhora a eficiência e facilita a implementação de novas funcionalidades.

4.3.3 Implementação e Desafios

Embora o HL7 FHIR ofereça uma solução poderosa para interoperabilidade, sua implementação requer atenção a desafios como:

- **Conformidade com Regulamentações:** Garantir que a troca de dados esteja em conformidade com normas como **HIPAA**, **GDPR** e **LGPD**.
- **Segurança e Privacidade:** Implementar mecanismos robustos de autenticação e criptografia para proteger os dados durante a troca entre sistemas.
- **Compatibilidade de Versões:** Assegurar que sistemas diferentes utilizem versões compatíveis do HL7 FHIR para evitar problemas de interoperabilidade.

Capítulo 5

Implementação e Testes

5.1 Implementação da Prova de Conceito

Todos os requisitos propostos no **Capítulo 3** foram implementados com sucesso. A seguir, são apresentados exemplos de trechos de código que retratam a implementação das funcionalidades mais críticas:

5.1.1 Restrição de Acesso com Base na Autenticação e no Papel do Utilizador

Há páginas acessíveis apenas para utilizadores não autenticados (deslogados) e outras que exigem que o utilizador esteja autenticado e possua um dos dois papéis: profissional ou utente. Isso foi alcançado por meio da correta configuração das rotas, juntamente com a implementação de *guards* (proteções de rotas) apropriadas.

Declaração das rotas:

```
../../../../src/app/app.routes.ts
...
// rotas para utilizadores deslogados (não autenticados)
{path: 'login', component: LoginComponent, canActivate: [loginGuard
  ]},
{path: 'register', component: RegisterComponent, canActivate: [
  loginGuard]},
// rotas para utilizadores logados (autenticados)
{path: 'home-patient', component: HomePatientComponent, canActivate
  : [authGuard], data: { role: 'patient' }},
{path: 'patient-professionals', component:
  PatientProfessionalsComponent, canActivate: [authGuard], data: {
  role: 'patient' }},
{path: 'patient-logs', component: PatientLogsComponent, canActivate
  : [authGuard], data: { role: 'patient' }},
{path: 'home-professional', component: HomeProfessionalComponent,
  canActivate: [authGuard], data: { role: 'professional' }},
{path: 'view-patient/:id', component: ViewPatientComponent,
  canActivate: [authGuard], data: { role: 'professional' }},
{path: '**', redirectTo: 'home-patient'}
...
```

Proteção de páginas acessíveis apenas a utilizadores não autenticados:

```

//./src/app/guards/login.guard.ts
...
const username = await firstValueFrom(_authState.pipe(map(u => u?.
  email)));
if (!username) {
  return true;
}

// utilizadores logados (autenticados) são redirecionados à página
  inicial correspondente aos papéis de cada um
const isUserProfessional = await userService.isUserProfessional(
  username);
const homePath = router.parseUrl(`/home-${ isUserProfessional ? "
  professional" : "patient" }`);
return new RedirectCommand(homePath);
...

```

Proteção de páginas para utilizadores autenticados com o papel adequado:

```

//./src/app/guards/auth.guard.ts
...
const username = await firstValueFrom(_authState.pipe(map(u => u?.
  email)));
if (!username) {
  // utilizadores deslogados (não autenticados) são
    redirecionados à página de autenticação
  const loginPath = router.parseUrl("/login");
  return new RedirectCommand(loginPath);
}
if (next.data["role"]) {
  // utilizadores sem o papel requerido são redirecionados à
    página inicial correspondente ao seu papel
  const isUserProfessional = await userService.isUserProfessional
    (username);
  if ((next.data["role"] === "professional") ? !isUserProfessional
    : isUserProfessional) {
    const homePath = router.parseUrl(`/home-${
      isUserProfessional ? "professional" : "patient" }`);
    return new RedirectCommand(homePath);
  }
}
return true;
...

```

5.1.2 Cifragem/Decifragem das Informações

A cifragem/decifragem das informações foi implementada por meio de um *service* (classe de serviço) dedicado exclusivamente a esse fim:

```
//./src/app/services/crypt.service.ts
export class CryptService {
  private readonly reservedKeys = [ 'id', 'lastLogin' ];

  encryptString(data: string): string {
    if (!data?.length) return data;
    return CryptoJS.AES.encrypt(data, environment.aesKey).toString()
  }

  encryptObject(object: any, excludes: string[] = []): any {
    const encryptedObject: any = {};
    for (let key of Object.keys(object)) {
      encryptedObject[key] = (this.reservedKeys.concat(excludes).includes(key)) ? object[key] : this.encryptString(object[key]);
    }
    return encryptedObject;
  }

  decryptString(data: string): string {
    if (!data?.length) return data;
    const bytes = CryptoJS.AES.decrypt(data, environment.aesKey);
    return bytes.toString(CryptoJS.enc.Utf8);
  }

  decryptObject(encryptedObject: any, excludes: string[] = []): any {
    {
      const object: any = {};
      for (let key of Object.keys(encryptedObject)) {
        object[key] = (this.reservedKeys.concat(excludes).includes(key)) ? encryptedObject[key] : this.decryptString(encryptedObject[key]);
      }
      return object;
    }
  }
}
```

5.1.3 Logs de Auditoria

Os logs de auditoria foram implementados por meio de um *service* (classe de serviço) dedicado exclusivamente a esse fim, e podem ser visualizados no Firestore pelos administradores do sistema através da interface de utilizador do Firebase, conforme demonstrado na Figura 5.1.

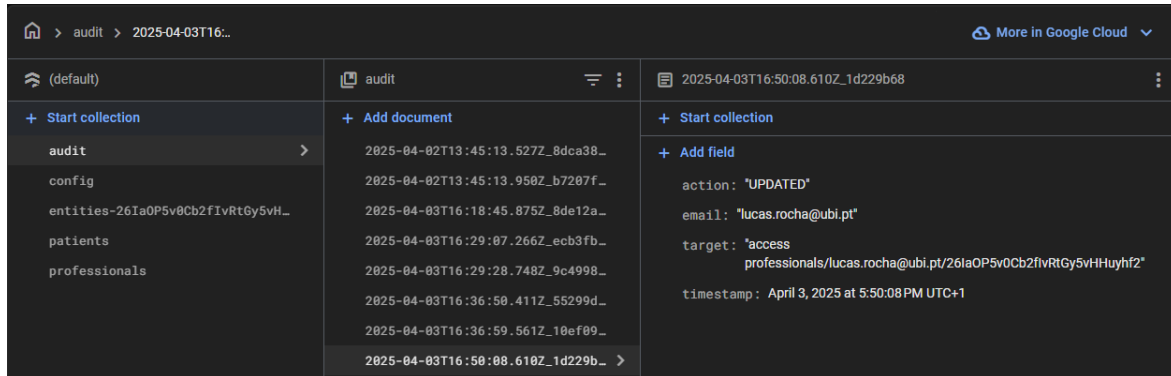


Figura 5.1: Logs de Auditoria

```

./src/app/services/logger.service.ts
export class LoggerService {
  private userService = inject(UserService);
  private firestore = inject(Firestore);
  private auditCollection: any;
  private email: string = '';

  constructor() {
    this.auditCollection = collection(this.firestore, 'audit');
    this.userService.getUserObservable().subscribe(user => {
      if (!user?.email) return;
      this.email = user.email;
    });
  }

  log(action: ACTION_TYPES, target: string) {
    const email = this.email;
    const timestamp = new Date();
    const logId = `${timestamp.toISOString()}_${window.crypto.
      randomUUID().substring(0, 8)}`;
    setDoc(doc(this.auditCollection, logId), {
      email,
      timestamp,
      action,
      target
    });
  }
}

```

```
}  
}
```

Exemplo de consumo (utilização) dos serviços de cifragem e logs de auditoria:

```
//./src/app/services/entity.service.ts  
...  
addEntity(entity: any) {  
    // encriptação (cifragem) das informações cadastradas pelo  
    // utilizador  
    const encryptedEntity = this.cryptService.encryptObject(entity)  
    ;  
    const promise = addDoc(this.entityCollection, encryptedEntity);  
    // registro do cadastro de um novo evento por parte do  
    // utilizador nos logs de auditoria  
    promise.then((docRef) => this.loggerService.log(ACTION_TYPES.  
        CREATED, 'entity ${this.entitiesCollectionId}/${docRef.id}'))  
    ;  
    return promise;  
}  
  
deleteEntity(entity: any) {  
    const target = `${this.entitiesCollectionId}/${entity.id}`;  
    // registra exclusão de evento por parte do utilizador nos  
    // logs de auditoria  
    deleteDoc(doc(this.firestore, target)).then(() => this.  
        loggerService.log(ACTION_TYPES.CREATED, 'entity ${target}'))  
    ;  
}  
...
```

5.1.4 Restrição de Acesso aos Dados de Utentes


Profissionais de saúde que tentem acessar dados de utentes sem a devida autorização, seja de forma intencional ou acidental, são automaticamente redirecionados à página inicial. Utentes recebem notificações dos acessos bem sucedidos (Figura 5.2).

```
//./src/app/components/view-patient/view-patient.component.ts  
...  
const data = this.patientService.getPatientsFromProfessional(  
    professional);  
// descriptação (decifragem) das permissões de acesso do  
// professional
```

```

const decryptedData: Access[] = data.map(access => this.
    cryptService.decryptObject(access));
const access = decryptedData.find(p => p.id === patientId && p.
    patientAcceptedAt && p.professionalAcceptedAt);
// redirecionamento à página inicial, caso o acesso não esteja
    devidamente autorizado
if (!access) {
    pelo utente
    this.router.navigateByUrl(homePath);
    return;
}
this.patientEmail = access.email;
// registro de acesso às informações para posterior visualização
    por parte do utente
this.patientService.logAccess(patientId, professional.id);
...

```

Menu	ubi-patient 
Meus eventos	Acessos às Minhas Informações
Meus profissionais	Filtrar
Logs de acesso	
Sair	

Data	Profissional
03/04/2025 19:50	lucas.rocha@ubi.pt
03/04/2025 16:50	lucas.rocha@ubi.pt
03/04/2025 16:50	lucas.rocha@ubi.pt
03/04/2025 16:50	lucas.rocha@ubi.pt
03/04/2025 14:12	lucas.rocha@ubi.pt
03/04/2025 13:51	lucas.rocha@ubi.pt
03/04/2025 13:44	lucas.rocha@ubi.pt
03/04/2025 13:43	lucas.rocha@ubi.pt
03/04/2025 13:40	lucas.rocha@ubi.pt
03/04/2025 13:39	lucas.rocha@ubi.pt
02/04/2025 12:31	lucas.rocha@ubi.pt
01/04/2025 16:51	lucas.rocha@ubi.pt
28/03/2025 13:49	lucasubi11813@gmail.com
28/03/2025 13:48	lucasubi11813@gmail.com
28/03/2025 13:44	lucasubi11813@gmail.com

Figura 5.2: Visualização de Acessos às Informações do Utente

5.2 Testes de Usabilidade

Para avaliar a qualidade da aplicação do ponto de vista dos utilizadores finais, foram realizados testes de usabilidade com um grupo de **6 participantes beta**, incluindo **4 utentes** e **2 profissionais de saúde**. A diversidade de perfis incluiu programadores, psicólogos clínicos e um balconista, com idades entre 27 e 36 anos.

A aplicação foi utilizada em diferentes dispositivos (smartphones, notebooks e ambos), durante períodos que variaram entre uma semana e um mês, nas proporções demonstradas pelos gráficos das figuras A.2 e A.3.

5.2.1 Resultados Quantitativos

Os participantes avaliaram a aplicação em diferentes dimensões, utilizando uma escala de 1 a 5. Os resultados médios foram:

- **Facilidade no acompanhamento do tratamento (figuras A.7 e A.11):** 4.7
- **Eficácia na gestão de informações (figura A.8):** 4.75
- **Eficácia no partilhamento de informações (figura A.9):** 5
- **Segurança e privacidade das informações dos utentes (figuras A.10 e A.12):** 4.2
- **Facilidade de uso: (figura A.4)** 4.5
- **Design da aplicação: (figura A.5)** 4.3
- **Qualidade técnica percebida: (figura A.6)** 4.8

5.2.2 Resultados Qualitativos

Os comentários recolhidos incluíram:

- Problemas técnicos identificados e corrigidos: ausência de validação do tamanho máximo suportado para imagens e partilhamento incorreto de dados entre contas em cenários de teste.
- Sugestões funcionais: adição de lembretes personalizados, histórico de doenças, medições de uso contínuo e envio de mensagens directamente ao utente.

5.2.3 Análise dos Resultados

Os resultados mostram que a aplicação foi bem recebida tanto por utentes quanto por profissionais. As sugestões recebidas são valiosas e serão consideradas em ciclos futuros de desenvolvimento. Todos os participantes consentiram formalmente com a utilização de suas respostas para fins de pesquisa académica. Representações gráficas detalhadas dos resultados obtidos podem ser encontradas no Anexo A.3.

Capítulo 6

Trabalhos Futuros e Conclusões

6.1 Trabalhos Futuros

Embora a solução proposta aborde aspectos fundamentais de gestão e segurança de informações de saúde, há espaço para melhorias e expansões que podem potencializar sua utilidade e alcance. Dentre os principais caminhos para trabalhos futuros, destacam-se:

6.1.1 Gamificação e Incentivos Comportamentais

A **gamificação** tem sido amplamente utilizada em diversos setores para aumentar o engajamento e a adesão dos usuários a determinadas atividades [3]. No contexto da saúde digital, a aplicação de técnicas de gamificação pode incentivar os **utentes** a monitorar sua própria saúde de maneira mais ativa, promovendo melhores hábitos e adesão a tratamentos médicos. Dentre os principais elementos de gamificação que podem ser incorporados à aplicação, destacam-se:

- **Sistemas de Recompensa:** Os **utentes** podem acumular pontos ou receber distintivos ao completar tarefas, como registrar sintomas diariamente, seguir um plano de medicação ou realizar consultas médicas regulares.
- **Desafios Personalizados:** Criar metas e desafios semanais ou mensais para incentivar o acompanhamento da saúde, como manter a pressão arterial dentro de níveis ideais ou atingir metas de atividade física.
- **Feedback Instantâneo:** Fornecer relatórios interativos e notificações motivacionais para manter o **utente** engajado e informado sobre seu progresso.
- **Rankings e Comunidades:** Criar mecanismos que permitam aos **utentes** comparar seu progresso com grupos de apoio ou familiares, promovendo um senso de comunidade e engajamento social.
- **Recompensas Tangíveis:** Explorar parcerias com farmácias, clínicas ou seguradoras para oferecer descontos ou benefícios aos **utentes** que mantêm bons hábitos de saúde.

A implementação dessas estratégias pode contribuir significativamente para a **adesão ao tratamento**, especialmente para **doenças crônicas**, onde a disciplina no acompanhamento médico e no uso de medicamentos é essencial. Além disso, a gamificação pode melhorar a experiência do usuário na aplicação, tornando-a mais interativa e intuitiva.

Para garantir a eficácia dessas técnicas, será necessário realizar estudos e testes com usuários reais, analisando métricas de engajamento e adaptando os incentivos de acordo com as

preferências dos **utentes**. A combinação de **gamificação com personalização baseada em IA** poderá levar a uma solução ainda mais eficiente e centrada no usuário.

Assim, a adoção da gamificação no projeto representa uma estratégia promissora para melhorar a adesão ao uso da plataforma e otimizar os resultados de saúde dos **utentes**.

6.1.2 Integração com Dispositivos de IoT

A integração com **dispositivos de Internet das Coisas (IoT)** representa uma oportunidade para ampliar as funcionalidades do sistema, permitindo o **monitoramento contínuo de sinais vitais**. Sensores conectados, como dispositivos vestíveis e monitores de glicose, poderiam capturar e transmitir dados em tempo real, enriquecendo o histórico clínico do utente e permitindo intervenções mais rápidas em casos críticos. Além disso, essa funcionalidade fomentaria a adoção de cuidados preventivos, proporcionando insights valiosos tanto para os utentes quanto para os profissionais de saúde.

6.1.3 Suporte a Dispositivos Médicos de Imagem via DICOM

A ampliação do sistema para suportar dispositivos médicos conectados por meio do padrão **DICOM (Digital Imaging and Communications in Medicine)** permitiria o armazenamento e a visualização de imagens médicas, como radiografias, tomografias e ressonâncias magnéticas. Essa integração possibilitaria que os profissionais de saúde acessassem imagens diagnósticas diretamente pelo sistema, promovendo uma experiência mais integrada e eficiente para a gestão de dados clínicos. A compatibilidade com DICOM facilitaria a interoperabilidade com equipamentos médicos amplamente utilizados em hospitais e clínicas.

6.1.4 Adição de um Backend Dedicado com Suporte a HL7 FHIR

Apesar de o sistema atual utilizar exclusivamente **Firestore** como backend-as-a-service (BaaS), a adição de um backend dedicado pode oferecer maior flexibilidade e controle. Não obstante, a implementação de interoperabilidade avançada com suporte ao padrão **HL7 FHIR** no backend pode proporcionar:

- Melhor integração com sistemas hospitalares e de farmácias para troca padronizada de informações de saúde.
- Processamento eficiente de dados clínicos complexos, como diagnósticos e prescrições.
- Gerenciamento mais granular das APIs para interoperabilidade com terceiros, permitindo maior personalização e compatibilidade.
- Implementação de lógica de negócios para validação e transformação de dados seguindo as especificações do HL7 FHIR.

A Figura 6.1 ilustra de maneira simplificada a diferença entre aplicações web tradicionais vs. BaaS.

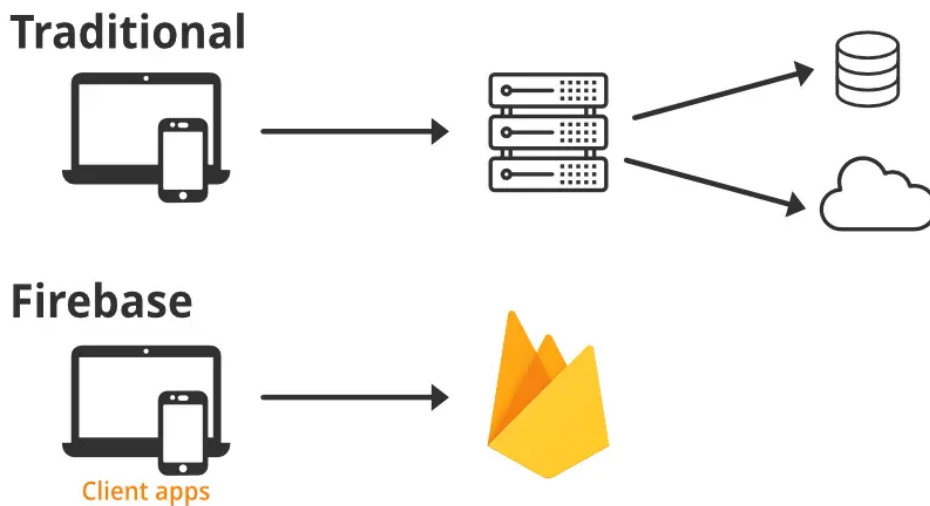


Figura 6.1: Firebase vs. Aplicação web tradicional

6.1.5 Exploração de Tecnologias Emergentes

Outra direção para trabalhos futuros inclui a exploração de **tecnologias emergentes**, como **Inteligência Artificial (IA)** e **Machine Learning (ML)**, para análise preditiva de dados. Esses algoritmos poderiam identificar padrões em históricos de saúde, auxiliando na detecção precoce de doenças e na personalização de tratamentos. Além disso, o uso de **blockchain** para garantir maior transparência e segurança nas transações de dados de saúde também é uma área promissora a ser investigada.

6.1.6 Testes Automatizados: Unit Tests, E2E e Mutation Testing

Uma importante melhoria futura para o sistema envolve a implementação de uma abordagem abrangente de testes automatizados, incluindo **Unit Tests**, **E2E (End-to-End) Testing** e **Mutation Testing**. Esses testes são fundamentais para garantir a qualidade do software, reduzir falhas em produção e aumentar a confiabilidade do sistema.

6.1.6.1 Unit Tests

Os **Unit Tests** são responsáveis por verificar o comportamento isolado de componentes ou funções individuais da aplicação. Eles garantem que cada unidade de código funcione corretamente conforme projetado. No contexto do sistema, os **Unit Tests** podem ser aplicados para:

- Verificar a lógica de cálculo e manipulação de dados no frontend.
- Validar regras de negócio implementadas, como validação de campos de formulários.
- Garantir que os métodos de interação com o **Firebase** retornem os resultados esperados.

Ferramentas como **Jest**, **Jasmine** e **Karma**, integradas ao Angular, podem ser utilizadas para desenvolver e executar os testes unitários.

6.1.6.2 E2E (End-to-End) Testing

Os testes **E2E** são projetados para verificar o comportamento do sistema como um todo, simulando interações do usuário e fluxos completos da aplicação. Esses testes garantem que todas as partes do sistema (frontend e backend) funcionem corretamente em conjunto. No projeto, os **E2E Tests** podem ser utilizados para:

- Simular fluxos de navegação, como cadastro e login de utentes.
- Verificar interações com formulários e listagens de dados.
- Garantir a funcionalidade de notificações e sincronizações de dados no PWA.

Para os testes E2E, ferramentas como **Cypress**, **Selenium** ou **Protractor** podem ser integradas ao pipeline de desenvolvimento.

6.1.6.3 Mutation Testing

O **Mutation Testing** é uma técnica avançada que introduz alterações deliberadas (ou "mutações") no código para avaliar a eficácia dos testes existentes. A ideia é verificar se os testes conseguem detectar as alterações inesperadas, indicando o quão robustos eles são. No contexto do sistema, o **Mutation Testing** pode ser útil para:

- Avaliar a qualidade dos **Unit Tests** e **E2E Tests**.
- Identificar partes do código que não estão cobertas adequadamente pelos testes existentes.
- Melhorar a cobertura e a confiabilidade dos testes automatizados.

Ferramentas como **Stryker Mutator** podem ser exploradas para implementar o Mutation Testing no projeto.

6.1.6.4 Impacto e Benefícios

A inclusão de testes automatizados no futuro desenvolvimento da aplicação trará os seguintes benefícios:

- **Redução de Erros:** Garantia de que funcionalidades críticas sejam testadas e validadas continuamente.
- **Manutenção Facilitada:** Identificação de regressões rapidamente durante o ciclo de desenvolvimento.
- **Maior Confiabilidade:** Melhor percepção de qualidade pelos usuários e maior confiança nas atualizações do sistema.

A implementação de uma estratégia robusta de testes automatizados será fundamental para a evolução do sistema, garantindo maior qualidade e suporte para expansões futuras.

6.1.6.5 Novas Funcionalidades

Implementação de novas funcionalidades sugeridas pelos utilizadores beta, como:

- Possibilidade de envio de mensagens directamente ao utente;
- Histórico de doenças (diagnósticos);
- Registro de medicações de uso contínuo.
- Adição de lembretes personalizados.

6.1.7 Resumo dos Próximos Passos

A evolução da aplicação concentra-se em ampliar sua funcionalidade, eficiência e alinhamento com as crescentes demandas do setor de saúde digital. Os trabalhos futuros visam consolidar a solução como uma ferramenta indispensável no ecossistema de saúde, por meio das seguintes iniciativas estratégicas:

- **Gamificação e incentivos comportamentais:** A utilização de recompensas, notificações e funcionalidades interactivas pode motivar os doentes a participarem mais ativamente no seu percurso de cuidados de saúde.
- **Integração com Dispositivos IoT:** Permitir o monitoramento contínuo de sinais vitais, utilizando sensores conectados para enriquecer o histórico clínico e viabilizar intervenções preventivas e ágeis.
- **Suporte a Padrões Médicos como DICOM:** Ampliar a interoperabilidade do sistema com dispositivos médicos, possibilitando o gerenciamento e a visualização de imagens diagnósticas diretamente na aplicação.
- **Internacionalização:** Adaptar a plataforma para ser utilizada globalmente, garantindo suporte a múltiplos idiomas, regulamentos locais e diferentes fusos horários. Permitindo que o sistema se adeque às necessidades culturais e legais de cada região, ampliando sua aplicação e alcance a nível mundial.
- **Backend Dedicado com suporte a HL7 FHIR:** Desenvolver um backend robusto que facilite a troca padronizada e segura de informações entre sistemas hospitalares, farmácias e a aplicação, promovendo maior interoperabilidade, flexibilidade e controle sobre os dados.
- **Automação de Testes Abrangentes:** Implementar uma estratégia completa de testes, incluindo Unit Tests, E2E Testing e Mutation Testing, para garantir alta confiabilidade, identificar regressões e facilitar a manutenção contínua.
- **Adoção de Tecnologias Emergentes:** Explorar soluções avançadas, como Inteligência Artificial para análise preditiva de dados e blockchain para assegurar transparência e integridade na gestão de informações sensíveis.

- **Implementação de novas funcionalidades** sugeridas pelos utilizadores beta, como: envio de mensagens directamente ao utente, histórico de doenças, registro de medicações de uso contínuo e adição de lembretes personalizados.

As melhorias sugeridas visam aprimorar a escalabilidade e inovação da solução, com foco nas necessidades dos utentes e profissionais de saúde. Espera-se que tais avanços impactem positivamente o setor, fomentando novas abordagens para o cuidado digital.

6.2 Conclusões

A gestão integrada de informações médicas representa um pilar fundamental para a transformação digital no setor de saúde. Este trabalho reforça a importância de ferramentas que não apenas centralizem os dados médicos, mas também coloquem o **utente** no centro da gestão de sua saúde, permitindo que ele tenha maior controle e visibilidade sobre suas informações clínicas.

A proposta apresentada visa criar uma solução que fomente a **colaboração eficiente entre utentes e profissionais de saúde**, facilitando a troca de informações de forma segura e padronizada. Essa integração promove um cuidado mais coordenado e personalizado, reduzindo erros, eliminando redundâncias, aumentando o engajamento e garantindo melhores resultados para os utentes.

Além disso, a utilização de padrões como **HL7 FHIR**, aliada a medidas de segurança robustas, como **criptografia de ponta a ponta** e **logs de auditoria**, assegura a proteção das informações sensíveis, construindo a confiança dos utentes e profissionais no sistema.

Por fim, ao adotar uma abordagem centrada na privacidade, interoperabilidade e usabilidade, esta aplicação tem o potencial de transformar a maneira como os dados de saúde são gerenciados e compartilhados, promovendo um ecossistema mais eficiente, inclusivo e seguro para todos os envolvidos.

Bibliografia

- [1] Stange, K. C. (2009). The problem of fragmentation and the need for integrative solutions. *Ann Fam Med.* 2, 9, 10
- [2] Jawad, L. A. (2024). Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. *Abhigyan.* 3, 6, 14, 29
- [3] Mwendwa, F. (2024). The Impact of Digital Health on Patient Engagement. *EEJPH Publications.* 2, 3, 13, 43
- [4] de Souza Ferreira, E., de Oliveira, A.H.M., Dias, M.A. et al. (2024). Mobile solution and chronic diseases: development and implementation of a mobile application and digital platform for collecting, analyzing data, monitoring and managing health care. *BMC Health Serv Res* 24. 3, 5, 10, 11
- [5] Department of Health and Human Services. (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Disponível em: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>. 7
- [6] European Parliament and Council of the European Union. (2018). General Data Protection Regulation (GDPR). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>. 8
- [7] Presidência da República do Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. 8, 9
- [8] Google. (2024). Angular - Official Website. Disponível em: <https://angular.io/> 15, 18
- [9] Google. (2024). Angular Material - Official Website. Disponível em: <https://material.angular.io/> 16, 18
- [10] Google. (2024). Firebase - Official Website. Disponível em: <https://firebase.google.com/> 16, 17, 18, 19
- [11] Atlassian. (2024). What is Agile? Disponível em: <https://www.atlassian.com/agile> 24, 25
- [12] Trello. (2024). What is Trello? Disponível em: <https://trello.com/tour> 25, 26
- [13] GitHub. (2024). About GitHub. Disponível em: <https://github.com/about> 21, 22
- [14] GitHub. (2024). Understanding GitHub Actions. Disponível em: <https://docs.github.com/en/actions/about-github-actions/understanding-github-actions> 22, 23
- [15] Sngular. (2025). Firebase: An all-in-one platform for Web and Mobile application development. Disponível em: <https://www.sngular.com/insights/313/firebase> 16

Apêndice A

Anexos

A.1 Requisitos do Sistema

A aplicação foi desenvolvida com base nos seguintes requisitos funcionais e não funcionais, visando atender às demandas específicas do projeto. Todo o desenvolvimento foi conduzido de acordo com o cronograma detalhado na Tabela A.1, garantindo a organização e o cumprimento das etapas dentro dos prazos estabelecidos.

Abaixo estão listados os requisitos funcionais e não funcionais para a aplicação proposta, organizados por categoria:

A.1.1 Gerenciamento de Utilizadores

- Implementação de autenticação com **Firebase**.
- Adição de suporte a **Cloud Firestore** para o armazenamento de dados.
- Implementação de controle de acesso baseado em papéis (**Role-Based Access Control - RBAC**).
- Adição dos seguintes papéis ao sistema:
 - **Utentes**;
 - **Profissionais de saúde**.

A.1.2 Funcionalidades para Utentes

- Utentes podem **cadastrar** informações como:
 - Alergias;
 - Cirurgias;
 - Cosméticos;
 - Exames;
 - Hervanárias;
 - Intolerâncias;
 - Medicações;
 - Medições;
 - Procedimentos;
 - Sintomas.

- Utentes podem **listar**, **visualizar** e **excluir** as informações cadastradas.
- Utentes podem **convidar profissionais de saúde** para visualizar seus dados.
- Utentes podem **aceitar ou rejeitar solicitações de acesso** feitas por profissionais de saúde.

A.1.3 Funcionalidades para Profissionais de Saúde

- Profissionais de saúde podem **solicitar acesso** aos dados dos utentes.
- Profissionais de saúde podem **aceitar ou rejeitar convites** enviados pelos utentes.
- Profissionais de saúde podem **listar os utentes** aos quais têm acesso.
- Profissionais de saúde podem **visualizar os dados individuais** de um utente ao selecionar o nome na lista de utentes com acesso.
- Profissionais de saúde podem **visualizar detalhes enviados pelos utentes**, como medicações, sintomas e outros, clicando nos itens específicos da lista.

A.1.4 Notificações

- Utentes devem **receber notificações** sempre que seus dados forem acessados por profissionais de saúde.

A.1.5 Requisitos Não Funcionais

- Implementação de **logs de auditoria** para rastrear acessos e modificações de dados, garantindo rastreabilidade.
- Proteção dos dados por meio de **criptografia de ponta a ponta**, tanto em repouso quanto em trânsito.
- Transformação da aplicação em **Progressive Web App (PWA)**, permitindo instalação em dispositivos, atualizações automáticas e design responsivo.
- Conformidade com regulamentações de privacidade de dados, incluindo **HIPAA**, **GDPR** e **LGPD**.
- **Internacionalização (i18n)**: A aplicação deverá oferecer uma interface multilíngue, com pelo menos dois idiomas: **português e inglês**, permitindo que os utilizadores possam interagir com o sistema em seu idioma nativo.

A.2 Cronograma de Desenvolvimento

O cronograma a seguir detalha as principais etapas do desenvolvimento do sistema utilizando **Angular** para o frontend e **Firebase** para serviços backend-as-a-service (BaaS), distribuído em 6 meses. A Figura A.1 representa uma versão simplificada do cronograma em formato de diagrama de Gantt.

Tabela A.1: Cronograma de Desenvolvimento

Período	Tarefa	Comentário
1º Mês	Planejamento e Configuração Inicial	Definição de requisitos, arquitetura e estrutura do projeto. Configuração inicial do Angular e integração com Firebase , incluindo autenticação, Firestore, Hosting e Storage.
2º Mês	Desenvolvimento da Interface do Usuário	Criação da interface do usuário com Angular Material , garantindo responsividade e usabilidade para web e dispositivos móveis. Implementação das telas principais, como cadastro, login e painel de utente.
3º Mês	Implementação de Funcionalidades	Adição de funcionalidades de cadastro, listagem, edição e exclusão de dados dos utentes (ex.: medicações, sintomas, alergias). Conexão com o Cloud Firestore para armazenamento em tempo real.
4º Mês	Integração com Padrões e Recursos Avançados	Implementação de suporte ao HL7 FHIR para integração com sistemas de saúde e adição de logs de auditoria para rastrear acessos e modificações. Configuração do sistema como PWA , permitindo funcionamento offline e instalação em dispositivos.
5º Mês	Testes e Validação	Realização de testes funcionais, de segurança e usabilidade para garantir a qualidade do sistema. Testes de autenticação, permissões e armazenamento no Firestore . Validação com utentes e profissionais de saúde para feedback.
6º Mês	Deploy e Ajustes Finais	Deploy no Firebase Hosting com monitoramento contínuo. Coleta de feedback inicial dos usuários e implementação de ajustes finais para refinar a experiência e corrigir possíveis problemas.

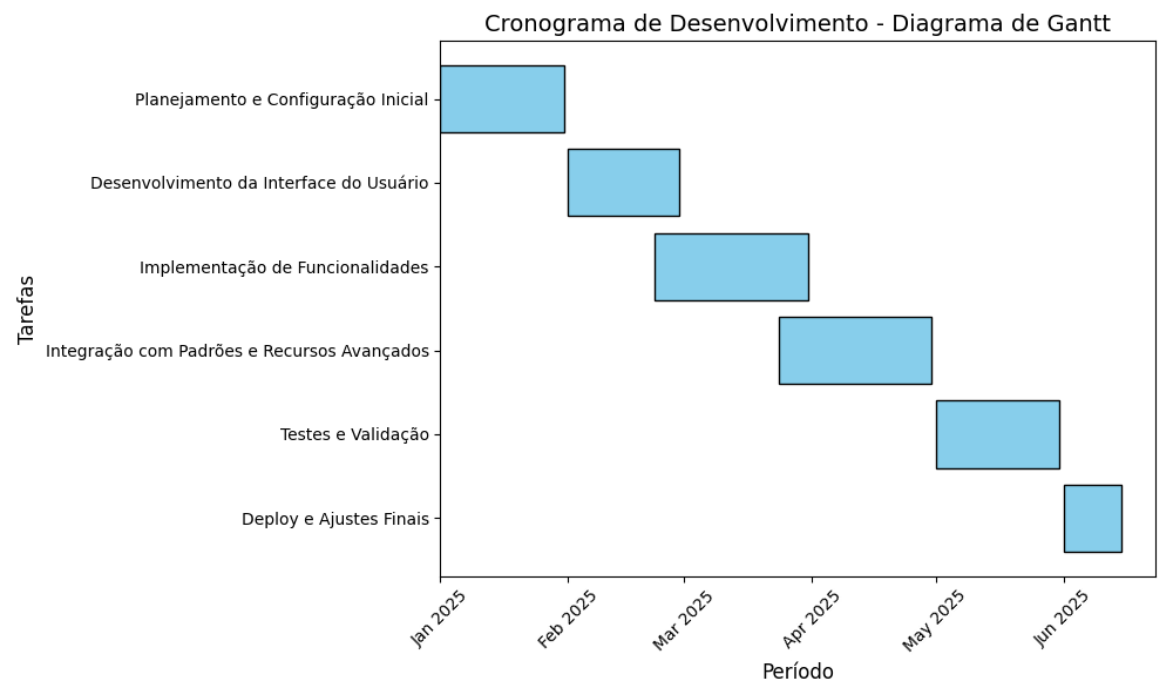


Figura A.1: Cronograma de Desenvolvimento - Diagrama de Gantt

A.3 Representações Gráficas dos Resultados dos Testes de Usabilidade

Em que tipo de dispositivo utilizou a aplicação?

6 respostas

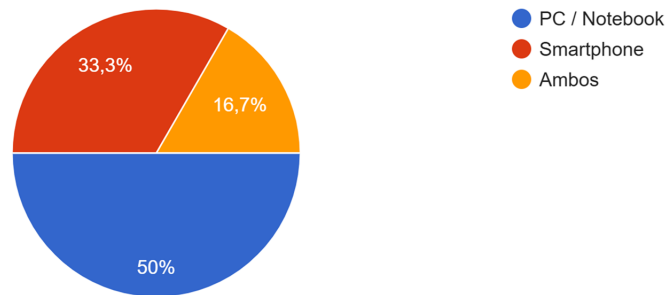


Figura A.2: Em que tipo de dispositivo utilizou a aplicação?

Por quanto tempo utilizou a aplicação?

6 respostas

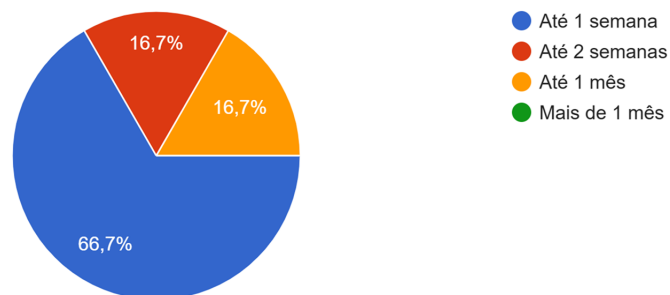


Figura A.3: Por quanto tempo utilizou a aplicação?

De 1 a 5, quão fácil e intuitiva foi a utilização da aplicação?

6 respostas

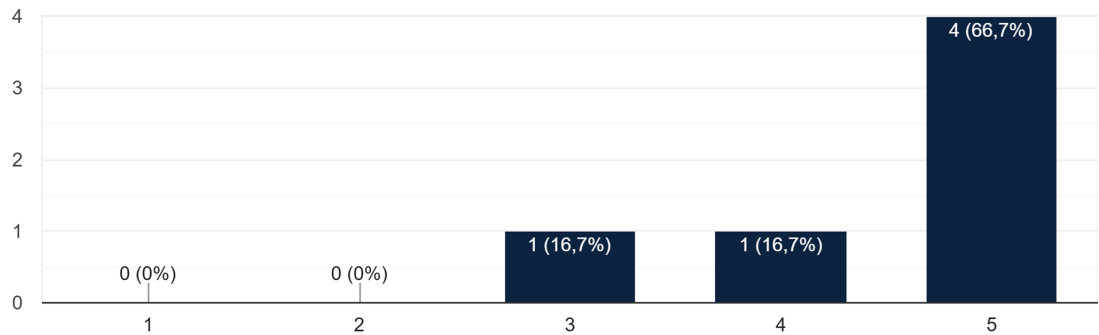


Figura A.4: Quão fácil e intuitiva foi a utilização da aplicação?

De 1 a 5, que nota daria ao design da aplicação?

6 respostas

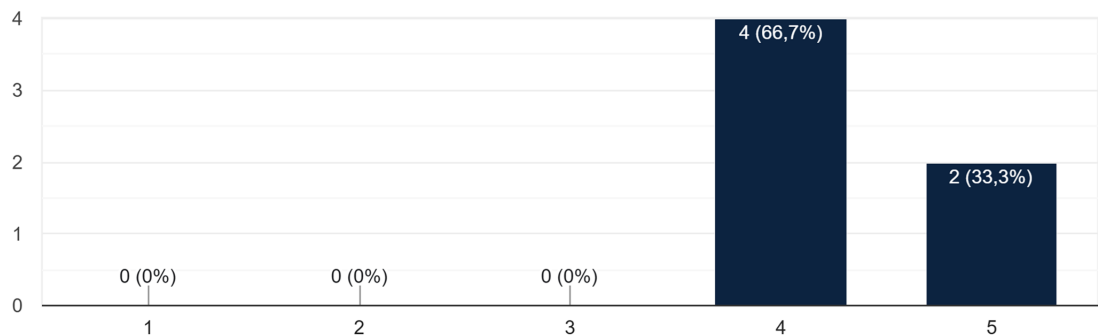


Figura A.5: Que nota daria ao design da aplicação?

De 1 a 5, que nota daria à qualidade técnica da aplicação?

6 respostas

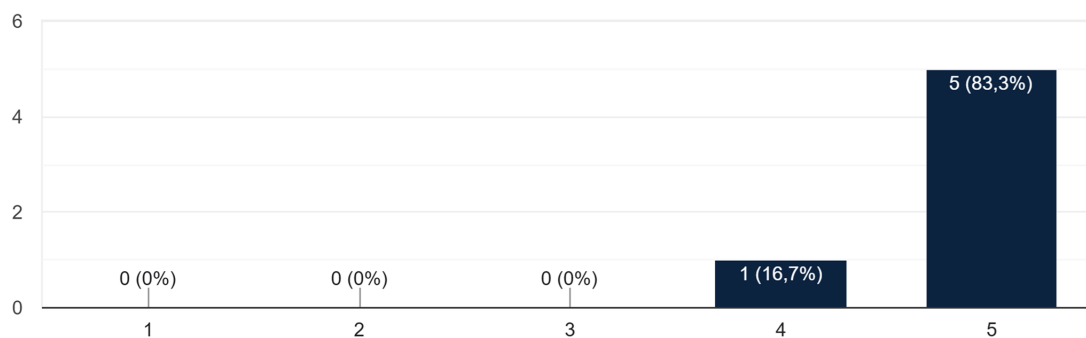


Figura A.6: Que nota daria à qualidade técnica da aplicação?

De 1 a 5, quanto a aplicação facilitou o acompanhamento e execução do tratamento?

4 respostas

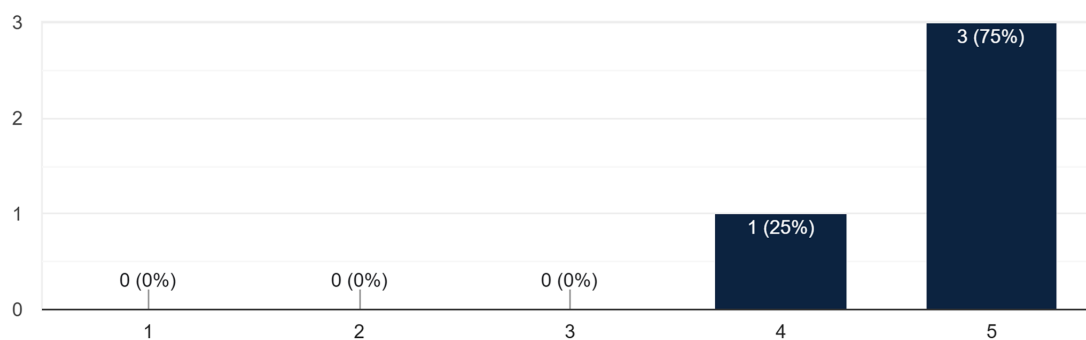


Figura A.7: A aplicação facilitou o acompanhamento e execução do tratamento?

De 1 a 5, qual a eficácia da aplicação na gestão das suas informações?

4 respostas

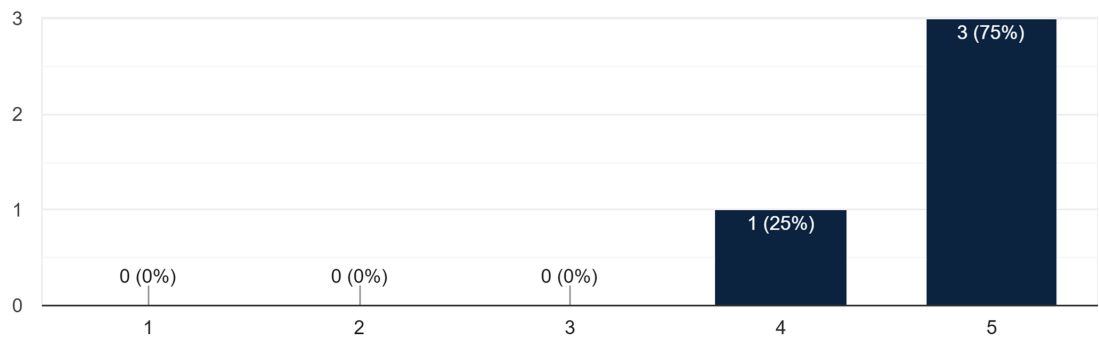


Figura A.8: Qual a eficácia da aplicação na gestão das suas informações?

De 1 a 5, qual a eficácia da aplicação no partilhamento das suas informações com profissionais de saúde?

4 respostas

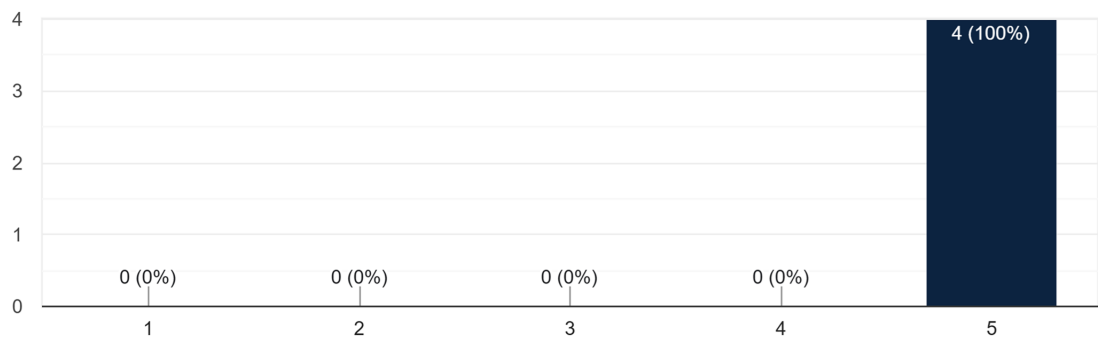


Figura A.9: Qual a eficácia da aplicação no partilhamento das suas informações com profissionais de saúde?

De 1 a 5, qual o seu nível de confiança na segurança e privacidade das suas informações na aplicação?

4 respostas

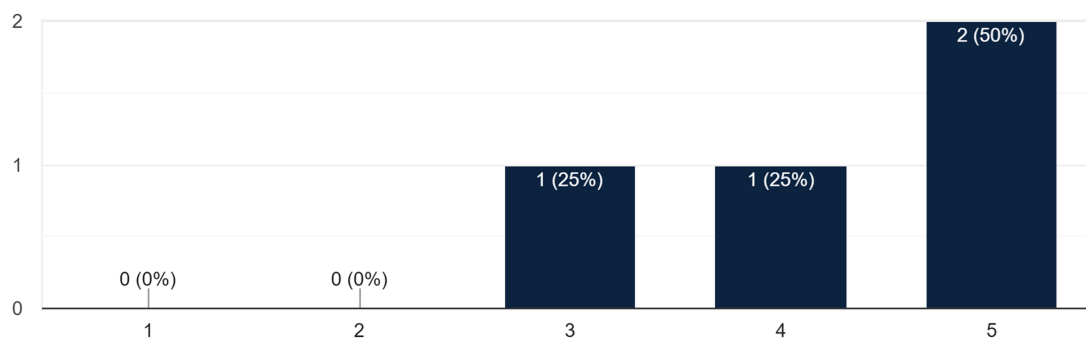


Figura A.10: Qual o seu nível de confiança na segurança e privacidade das suas informações na aplicação?

De 1 a 5, qual a eficácia da aplicação no acompanhamento de utentes (pacientes)?

2 respostas

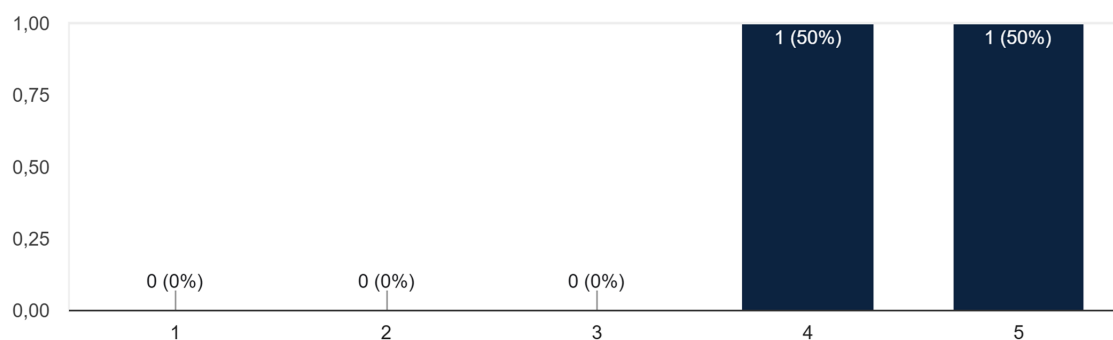


Figura A.11: Eficácia da aplicação no acompanhamento de utentes.

De 1 a 5, qual o seu nível de confiança na segurança e privacidade das informações dos utentes (pacientes) na aplicação?

2 respostas

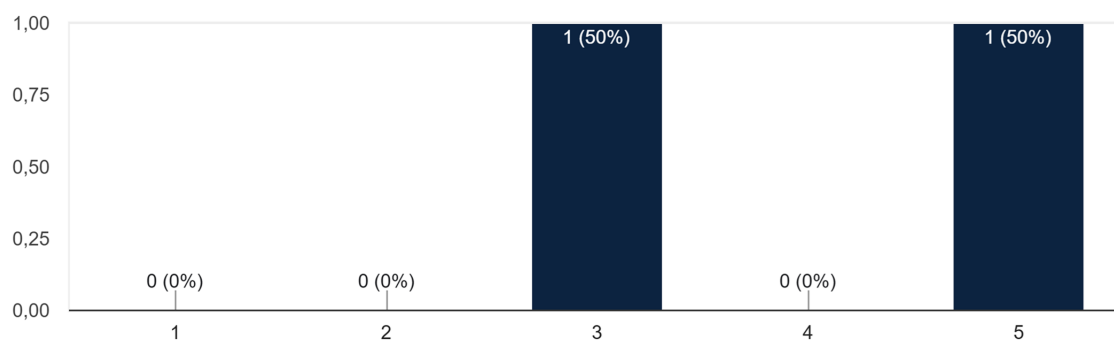


Figura A.12: Nível de confiança na segurança e privacidade das informações dos utentes.

Glossário

2FA	<i>Two-Factor Authentication</i> , mecanismo de autenticação que adiciona uma camada extra de segurança ao exigir duas formas de verificação antes de conceder acesso ao usuário.
AES	<i>Advanced Encryption Standard</i> , um algoritmo de criptografia amplamente utilizado para garantir a segurança de dados em sistemas digitais.
Angular	Framework front-end desenvolvido pelo Google para criação de aplicações web modernas e responsivas.
AWS	Amazon Web Services, plataforma de computação em nuvem que oferece uma ampla gama de serviços, incluindo armazenamento, computação e banco de dados.
Azure	Plataforma de computação em nuvem da Microsoft que fornece serviços como hospedagem, banco de dados, autenticação e integração com o ecossistema Microsoft.
BaaS	<i>Backend-as-a-Service</i> , modelo de serviço em nuvem que fornece ferramentas e infraestrutura pronta para autenticação, banco de dados, armazenamento e outras funcionalidades, permitindo que os desenvolvedores foquem no frontend.
CI/CD	Continuous Integration (Integração Contínua) e Continuous Deployment (Entrega Contínua), práticas DevOps que automatizam testes, integração e entrega de software para acelerar o desenvolvimento e aumentar a confiabilidade.
DICOM	Digital Imaging and Communications in Medicine, padrão utilizado para armazenamento e troca de imagens médicas, como radiografias e tomografias.
e-Health	Uso de tecnologias digitais e comunicação para melhorar o atendimento à saúde, promovendo acessibilidade e eficiência.
Firebase	Plataforma backend-as-a-service (BaaS) da Google que fornece ferramentas como autenticação, banco de dados em tempo real e hospedagem.
GDPR	General Data Protection Regulation, regulamento europeu que protege os dados pessoais e a privacidade dos cidadãos da União Europeia.
HIPAA	Health Insurance Portability and Accountability Act, uma legislação dos EUA que regula a privacidade e a segurança de informações de saúde.
HL7 FHIR	Fast Healthcare Interoperability Resources, um padrão que facilita a troca de dados de saúde entre sistemas de forma padronizada e segura.
IoT	Internet of Things, tecnologia que conecta dispositivos e sensores à internet para coleta e troca de dados em tempo real.

Ferramentas para integração de informação médica

LGPD	Lei Geral de Proteção de Dados, legislação brasileira que regula o tratamento de dados pessoais para garantir privacidade e transparência.
Logs de Auditoria	Registros detalhados de acessos e modificações de dados, utilizados para rastreamento e monitoramento de ações em sistemas.
Material Design	Sistema de design criado pelo Google, utilizado para desenvolver interfaces de usuário consistentes e acessíveis.
Node.js	Ambiente de execução JavaScript que permite o desenvolvimento de aplicações server-side, conhecido por sua alta performance e escalabilidade.
PWA	Progressive Web App, um aplicativo web que pode ser instalado em dispositivos e oferece funcionalidades semelhantes a aplicativos nativos.
Serverless	Modelo de computação em nuvem que permite executar código sob demanda sem a necessidade de gerenciar servidores, com escalabilidade automática e cobrança baseada no uso.
Supabase	Plataforma <i>open-source</i> baseada em PostgreSQL que fornece autenticação, banco de dados em tempo real e armazenamento como alternativa ao Firebase.
TLS	<i>Transport Layer Security</i> , protocolo criptográfico projetado para proteger dados transmitidos pela internet, garantindo confidencialidade, integridade e autenticidade da comunicação.