UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE DO CAMPUS ARARANGUÁ
CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

Raphael Abreu Farias de Jesus

Segurança Mobile: Desafios e Soluções em Aplicativos Móveis na Área da Saúde

Araranguá
2024

Raphael Abreu Farias de Jesus

Segurança Mobile: Desafios e Soluções em Aplicativos Móveis na Área da Saúde

Trabalho de Conclusão de Curso do Curso de Graduação em Engenharia de Computação submetido ao Centro de Ciências, Tecnologias e Saúde do Campus Araranguá da Universidade Federal de Santa Catarina para a obtenção do título de Bacharel em Engenharia de Computação.
Orientadora: Profa. Analúcia Schiaffino Morales, Dra.

Araranguá
2024

Raphael Abreu Farias de Jesus

Segurança Mobile: Desafios e Soluções em Aplicativos Móveis na Área da Saúde

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Engenharia de Computação e aprovado em sua forma final pelo Curso de Graduação em Engenharia de Computação.

Araranguá, 28 de Junho de 2024.

Prof. Jim Lau, Dr.
Coordenador do Curso

Banca Examinadora:

Profa. Analúcia Schiaffino Morales, Dra.
Orientadora

Prof. Alison Roberto Panisson, Dr.
Avaliador
Universidade Federal de Santa Catarina

Prof. Jim Lau, Dr.
Avaliador
Universidade Federal de Santa Catarina

Segurança Mobile: Desafios e Soluções em Aplicativos Móveis na Área da Saúde

Raphael Abreu Farias de Jesus* Analúcia Schiaffino Morales †

2024, JUNHO

Resumo

O crescente uso de tecnologias móveis na saúde tem impulsionado avanços significativos na gestão do cuidado ao paciente, porém levanta questões críticas sobre a segurança e a privacidade dos dados. Neste contexto, este estudo aborda os desafios e soluções para a segurança e privacidade em aplicativos móveis de saúde, destacando a importância da integração de práticas de Privacy by Design (PbD) desde a fase de desenvolvimento. Através da implementação de um framework em Flutter, a metodologia adotada foca na implementação de medidas de proteção de dados sensíveis, como medidas de prevenção contra capturas de tela e a criptografia de dados, visando uma conformidade rigorosa com normativas como a Lei Geral de Proteção de Dados (LGPD). Os resultados demonstram que a adoção de PbD não só atende aos requisitos legais, mas também fortalece a confiança dos usuários ao proteger de forma eficaz seus dados pessoais. Conclui-se que o framework proposto pode estabelecer um novo padrão para o desenvolvimento de aplicativos móveis de saúde, garantindo que segurança e privacidade sejam integralmente consideradas em todas as etapas do processo de design e operação dos aplicativos.

Palavras-chave: segurança, privacy by design, LGPD, aplicativo móvel.

*raphaelrat@hotmail.com
†analucia.morales@ufsc.br

Mobile Security: Challenges and Solutions in Health Care Applications

Raphael Abreu Farias de Jesus* Analúcia Schiaffino Morales †

2024, JUNHO

Abstract

The increasing use of mobile technologies in healthcare has driven significant advancements in patient care management, yet it raises critical issues regarding data security and privacy. In this context, this study addresses the challenges and solutions for security and privacy in mobile health applications, emphasizing the importance of integrating Privacy by Design (PbD) practices from the development phase. Through the implementation of a framework in Flutter, the adopted methodology focuses on implementing protective measures for sensitive data, such as prevention against screen captures and data encryption, aiming for strict compliance with regulations like the General Data Protection Law (LGPD). The results demonstrate that the adoption of PbD not only meets legal requirements but also strengthens user trust by effectively protecting their personal data. It is concluded that the proposed framework can establish a new standard for the development of mobile health applications, ensuring that security and privacy are comprehensively considered at all stages of the application design and operation process.

Key-words: security, privacy by design, GDPL, mobile application.

*raphaelrat@hotmail.com
†analucia.morales@ufsc.br

1 Introdução

Nos dias atuais, observa-se um grande avanço dos sistemas na área da saúde que englobam o conceito de *e-health* da Organização Mundial de Saúde, em que a Tecnologia da Informação auxilia a mediar a saúde dos indivíduos através de sistemas destinados à assistência ao paciente, avanços de pesquisa, educação e capacitação de profissionais de saúde, monitoração e avaliação em saúde (KEINERT; CORTIZO, 2018), torna-se necessário um cuidado redobrado com os dados dos pacientes e dos profissionais da saúde. Aliados ao crescimento da tecnologia, que inclui o uso de sensores, técnicas de inteligência artificial e mencanismos de comunicação para viabilizar os recursos necessários ao *e-health*, destaca-se neste contexto, a evolução e a disseminação dos aplicativos móveis, onde a digitalização dos processos de cuidado e monitoramento, tem contribuído significativamente para melhorar a acessibilidade e a eficácia dos serviços prestados. Especificamente, aplicativos móveis tem amplo alcance na área da saúde, tanto para os profissionais de saúde quanto para os pacientes. Os aplicativos *e-health* podem atender ambas as entidades. Em (PIRES et al., 2020) são classificados diversos aplicativos móveis para a saúde. Os autores identificam as seguintes classes de aplicativos utilizados por médicos: monitoramento e diagnóstico de pacientes, cuidados pessoais, saúde psicológica, educação e redes sociais. Além disso, os autores também classificaram aplicativos móveis usados por pacientes, como aplicativos de cuidados individuais (como por exemplo, esportes, jogos e diagnóstico), aplicativos para verificar seus batimentos cardíacos e calorias, aplicativos para entrar em contato com seu profissional de saúde, aplicativos educacionais de saúde e aplicativos de redes sociais.

Entretanto, o avanço da tecnologia e a transformação digital na área da saúde, implicam em desafios significativos relacionados à segurança e privacidade dos dados dos usuários. A natureza sensível das informações de saúde manipuladas por esses aplicativos ressalta a importância do desenvolvimento e implementação de medidas de segurança robustas para proteger contra ameaças digitais (GUDLUR, 2023). O *Privacy by Design* (PbD) é um conceito criado por Ann Cavoukian em 1990, que incorpora conceitos de privacidade no desenvolvimento de sistemas (CAVOUKIAN et al., 2009). Este conceito está alinhado à Lei Geral de Proteção de Dados (LGPD) e é também referenciado em outras normativas internacionais de privacidade. Esse princípio orienta que a proteção de dados pessoais deve ser considerada desde o início do desenvolvimento de qualquer sistema ou serviço, garantindo que a privacidade seja um elemento integrado e não um adicional. Este enfoque garante que a privacidade e a proteção de dados não sejam apenas um acréscimo, mas partes fundamentais do processo de desenvolvimento, aumentando assim a confiança dos usuários e a conformidade com a legislação vigente (LESCISIN; MAHMOUD, 2023). Além disso, a segurança em aplicativos móveis na área da saúde é crítica, dada a frequência crescente de ataques cibernéticos e violações de dados que comprometem a confidencialidade e a integridade das informações dos pacientes (ZANON et al., 2022). A necessidade de uma abordagem multidisciplinar para garantir a segurança dos dados dos usuários é evidenciada pelos desafios relacionados à segurança da rede, autenticação, ataques *Man-in-the-Middle* e conformidade regulatória (ALIASGARI; BLACK; YADAV, 2018).

Em particular, a LGPD ou Lei Nº 13.709 de 14 de agosto de 2018, estabeleceu um novo padrão em proteção de dados no Brasil, exigindo que as empresas adotem medidas eficazes para proteger as informações pessoais contra acessos não autorizados e vazamentos de dados. A conformidade com essa legislação é crucial, pois as penalidades por não cumprimento podem ser severas. A implementação dos conceitos de *Privacy by Design*

é, portanto, uma abordagem estratégica para atender às exigências da legislação vigente, integrando a segurança desde o projeto até a operação dos aplicativos móveis de saúde (XIONG et al., 2020). O objetivo do presente trabalho é o desenvolvimento de um *framework* em Flutter, designado a promover o PbD, que será útil tanto para plataformas Android quanto iOS voltado para a área da saúde. Será empregado código nativo, desenvolvido em Kotlin para Android e Swift para iOS, para chamar métodos nativos que garantem a adesão aos princípios fundamentais de privacidade. O estudo desenvolvido contribui para a literatura existente ao fornecer uma análise de vulnerabilidades de segurança em aplicativos móveis de saúde, e destacar as práticas recomendadas e tecnologias emergentes para fortalecer a segurança desses aplicativos. Através desta pesquisa, será oferecido *insights* valiosos para desenvolvedores, pesquisadores e profissionais de saúde, incentivando a adoção de uma cultura de segurança que priorize a proteção dos dados dos pacientes acima de tudo.

O presente artigo está organizado em sete seções. A Seção 2 apresenta um conjunto de trabalhos selecionados na literatura científica que estão relacionados com o *framework* desenvolvido. A Seção 3 destaca vulnerabilidades em aplicativos móveis junto com as premissas de segurança e as estratégias para melhoria da mesma. O *Privacy by Design* é tratado na seção 4. A Seção 5 descreve o desenvolvimento do *framework* e suas funcionalidades. Seguem a conclusão e as referências bibliográficas.

2 Trabalhos relacionados

Até alguns anos atrás, não havia tanta preocupação com os aspectos de segurança sob o ponto de vista regulatório. Relatos de trabalhos que apontavam a necessidade de recursos de segurança e privacidade na área da saúde, datam de períodos anteriores ao estabelecimento da LGPD no Brasil, como é o caso de (KEINERT; CORTIZO, 2018). Desta forma, a pesquisa para o desenvolvimento do presente trabalho inciou investigando os aplicativos móveis e as questões de regulação sobre segurança e privacidade e as práticas do PbD neste contexto. Foram investigados na literatura científica então, artigos relacionados ao trabalho. A seleção foi feita considerando as palavras-chaves: privacidade, segurança e aplicativos móveis na base de dados da IEEE Xplore. Os estudos escolhidos apresentaram aspectos relacionados à Lei Geral de Proteção de Dados, e ou, ao *General Data Protection Regulation* (GDPR) da União Européia.

Outro ponto investigado foram os conceitos de PbD e as premissas de segurança nos dispositivos móveis. Em uma rápida avaliação dos estudos percebe-se que os trabalhos são recentes, a seleção aponta estudos no período de 2019 a 2023. Os resultados ainda que incipientes, apresentam poucos resultados sobre o uso dessas normativas no desenvolvimento de aplicativos móveis, dos dez trabalhos selecionados disponíveis na Tabela 1, apenas um menciona regulação de lei geral de privacidade de dados (YAQUB et al., 2023) . E com relação ao PbD, dos dez artigos selecionados dois mencionaram a metodologia selecionada por este projeto (LI; YE, 2019) e (WIERINGA et al., 2021). Estes resultados evidenciam uma oportunidade de explorar mais profundamente os temas no desenvolvimento do presente trabalho.

Os artigos selecionados estão apresentados na Tabela 1 com uma breve descrição, sinalizando se eles têm referência à legislação sobre segurança e privacidae ou se eles são baseados nas recomendações do PbD. Observou-se uma carência de discussões profundas sobre a implementação de PbD em aplicativos móveis e no desenvolvimento de *software* em

Tabela 1 – Análise de Artigos sobre Privacidade e Segurança em Aplicativos Móveis

Artigo	**Descrição**	**Legis.**	**Privacy by Design**
(YAQUB et al., 2023)	Análise da conformidade de aplicativos de saúde com o GDPR e suas políticas de privacidade.	Sim	Não
(LI; YE, 2019)	Discussão sobre a implementação de privacidade diferencial local em coleta de dados móveis.	Não	Sim
(MHLANGA; MAITI; HAMMER, 2021)	Exploração das questões de segurança envolvendo dispositivos móveis e uso de mídias sociais.	Não	Não
(GARDNER et al., 2022)	Desenvolvimento de ferramentas para ajudar na criação de etiquetas de privacidade precisas em apps.	Não	Não
(ANIKEEV; SHULMAN; SIMO, 2021)	Avaliação da usabilidade e legibilidade das políticas de privacidade em aplicativos móveis.	Não	Não
(GUDLUR, 2023)	Discussão sobre desafios e vulnerabilidades de segurança em empresas de tecnologia financeira.	Não	Não
(ZHANG; SHAHRIAR; RIAD, 2020)	Análise de segurança e privacidade em dispositivos vestíveis de saúde.	Não	Não
(ALIASGARI; BLACK; YADAV, 2018)	Exame de vulnerabilidades de segurança em aplicações de saúde móveis e suas implicações.	Não	Não
(PRIAMBODO et al., 2022)	Avaliação de segurança em apps de saúde usando a lista OWASP Top 10 para vulnerabilidades móveis.	Não	Não
(WIERINGA et al., 2021)	Discussão sobre o equilíbrio entre análise de dados e privacidade em ambientes corporativos.	Não	Sim

Fonte: Próprio Autor

geral. Um único estudo identificou que, apesar da existência de regulamentações rigorosas como a LGPD e o GDPR, há uma aplicação limitada desses conceitos na prática, o que reforça a relevância deste trabalho. Além disso, esta breve revisão auxiliou na identificação das vulnerabilidades no desenvolvimento de aplicações móveis em saúde (PRIAMBODO et al., 2022), (ALIASGARI; BLACK; YADAV, 2018), descrita na próxima seção. A proposta

do presente estudo é propor diretrizes práticas para os desenvolvedores, incentivando a adoção de PbD desde as fases iniciais do desenvolvimento de novas aplicações. Essas diretrizes são fundamentadas pela análise de artigos recentes, demonstrando a necessidade de uma abordagem integrada e orientada pela privacidade na criação de aplicativos móveis seguros e confiáveis.

3 Segurança em Aplicativos Móveis

Esta seção aborda os desafios de segurança e privacidade em aplicativos móveis na área da saúde, destacando a importância de medidas robustas de segurança desde o início do desenvolvimento. Serão discutidas as vulnerabilidades comuns encontradas nesses aplicativos, além das premissas gerais de segurança.

3.1 Vulnerabilidades

Os aplicativos móveis na área da saúde são uma fronteira em constante expansão no uso da tecnologia moderna, permitindo que os usuários registrem dados de saúde, entrem em contato com seus médicos e se conectem a dispositivos médicos a partir de um smartphone. No entanto, essas aplicações enfrentam desafios significativos em termos de segurança e privacidade dos dados dos usuários. Uma análise realizada por (ALIASGARI; BLACK; YADAV, 2018) sobre vinte e cinco aplicações *mHealth* disponíveis na Google Play Store, revelou falhas em relação à conformidade com a HIPAA (*Health Insurance Portability and Accountability Act*), além de vulnerabilidades críticas de segurança e privacidade, incluindo problemas com segurança de rede, autenticação e vulnerabilidades a ataques *Man-in-the-Middle* .

A importância de garantir a segurança em aplicativos móveis é amplificada pela implementação da LGPD, que impõe rigorosas obrigações de proteção de dados pessoais, especialmente dados sensíveis como os de saúde. Violações de segurança que resultem em vazamentos de dados podem ter consequências devastadoras, não apenas em termos de penalidades legais, mas também no que diz respeito à perda de confiança do paciente e potencial dano à reputação das instituições de saúde. Portanto, é crítico adotar uma abordagem robusta de segurança desde o *design* até a operação dos aplicativos, garantindo que as medidas de proteção estejam integradas em todos os níveis do desenvolvimento e funcionamento dos sistemas.

Adicionalmente, um estudo sobre a segurança das aplicações *mHealth* com base nas 10 principais vulnerabilidades móveis da OWASP (*Open Web Application Security Project*) mostrou que todas as aplicações analisadas possuem vulnerabilidades de segurança e/ou privacidade (PRIAMBODO et al., 2022). Esse estudo destaca a importância de desenvolver técnicas eficientes de teste e avaliação de segurança para garantir a segurança desses sistemas complexos. Dentre as vulnerabilidades identificadas em aplicações móveis de saúde, destacam-se:

- Uso de algoritmos de criptografia fracos, como o SHA1, representando um risco de vazamento de informações.
- Presença de códigos rígidos sensíveis, indicando risco potencial de exploração por atacantes.

- Falhas de autenticação e autorização de usuários, permitindo acesso não autorizado a informações sensíveis dos usuários e a funções críticas da aplicação.
- Armazenamento inseguro de dados, que pode levar à exposição de informações confidenciais.
- Comunicação insegura, permitindo a interceptação de dados durante a transmissão.
- Falhas na autorização de usuários, possibilitando o acesso indevido a funções críticas da aplicação.
- Exposição a ataques de injeção de código, onde entradas maliciosas podem ser injetadas em uma aplicação, comprometendo a segurança do sistema.
- Inadequada gestão de sessões e cookies, que pode permitir ataques de sequestro de sessão, expondo os usuários a roubos de identidade.
- Vulnerabilidades em componentes de terceiros, como bibliotecas e *frameworks* desatualizados que podem ser explorados para ganhar acesso não autorizado ou executar código malicioso.
- Configurações de segurança inadequadas em plataformas móveis, permitindo que aplicativos acessem mais dados do que o necessário ou interfiram uns com os outros.
- Falhas na implementação de controle de acesso baseado em funções, permitindo que usuários com privilégios insuficientes executem ações que deveriam ser restritas.

3.2 Premissas de Segurança

A segurança em aplicações móveis tem se tornado cada vez mais crucial devido à natureza sensível dos dados manipulados por esses dispositivos. Com a crescente integração de aplicativos na área da saúde, as preocupações com a segurança e privacidade dos dados aumentam significativamente.

A proteção dos dados não é apenas uma questão de conformidade, mas também uma necessidade fundamental para garantir a confiança do paciente e a integridade do tratamento. As premissas de segurança são moldadas pela necessidade de manter a confidencialidade e integridade dos dados, ao mesmo tempo em que se garante a disponibilidade e autenticação apropriada (ZANON et al., 2022).

As premissas de segurança são fundamentais para projetar aplicações mais seguras e proteger os dados dos pacientes. Desta forma é possível melhorar as ferramentas propostas para auxiliar a área da saúde, bem como, melhorar a confiança nos sistemas destinados para a saúde. A seguir são descritas algumas das premissas de segurança associadas à saúde (MANOEL, 2022).

- **Confidencialidade:** Essencial para assegurar que as informações de saúde do paciente não sejam acessadas ou divulgadas indevidamente. A confidencialidade é mantida através de medidas como criptografia de dados e controles de acesso rigorosos.
- **Integridade:** Refere-se à precisão e consistência dos dados coletados e processados. A integridade é vital para garantir que os dados de saúde reflitam corretamente o estado do paciente e não sejam alterados ou corrompidos durante a transmissão ou armazenamento.

- **Não Repúdio:** Importante para assegurar a autenticidade das transações e prevenir que as partes envolvidas neguem suas ações. Isso é particularmente crítico em aplicações de saúde, onde a responsabilidade pelos dados e ações é um fator chave.
- **Autenticação:** Garante que apenas usuários autorizados possam acessar e interagir com o sistema. A autenticação efetiva é fundamental para prevenir acessos não autorizados e potenciais ataques.
- **Autorização:** Assegura que usuários tenham permissões apropriadas para acessar certos níveis de dados ou executar determinadas ações dentro do sistema. A autorização adequada é crucial para a governança de dados e controle de acesso.
- **Disponibilidade:** Refere-se à capacidade dos sistemas de estarem operacionais e acessíveis quando necessário, especialmente em situações de emergência médica. A alta disponibilidade é crucial para garantir que os cuidados de saúde não sejam interrompidos.

3.3 Estratégias para Melhoria da Segurança em Aplicativos Móveis

O cenário de segurança em aplicativos móveis é marcado por uma série de desafios complexos que são intensificados pela diversidade de dispositivos e sistemas operacionais, assim como pela natureza sensível dos dados processados. A necessidade de proteção contra acessos não autorizados requer uma abordagem abrangente e dinâmica para a segurança (ZHOU et al., 2021).

Para enfrentar esses desafios, é crucial adotar estratégias eficazes e abrangentes, como o desenvolvimento e implementação de processos de aplicação segura que incluem planejamento, *design*, desenvolvimento, teste e implantação. Estes processos devem focar na criação de *firewalls* robustos e na implementação de infraestruturas de rede seguras (GUDLUR, 2023). Adotar práticas de desenvolvimento seguro e realizar avaliações de segurança regulares são essenciais para manter a segurança dos dados e a integridade dos aplicativos móveis (PRIAMBODO et al., 2022).

Além da implementação de estruturas de segurança robustas, é crucial assegurar que a proteção dos dados esteja em conformidade com as exigências da LGPD, destacando a importância da criptografia de dados e a adesão às diretrizes do *Privacy by Design*, pois são vitais para evitar vazamentos e manter a segurança dos dados de todo tipo de usuário, seja esse com ou sem experiência, fortalecendo a segurança de aplicativos móveis de maneira abrangente, conforme as normativas legais (XIONG et al., 2020).

Adotar as práticas recomendadas de *Privacy by Design* significa integrar a proteção de dados em todas as etapas do desenvolvimento de aplicativos, desde a análise até a mitigação de riscos, passando pela concepção, implementação e operação do sistema. A implementação dessas práticas assegura que os aplicativos móveis atendam não apenas aos requisitos técnicos de segurança, mas também às expectativas legais e éticas de privacidade. Assim, a conformidade com a LGPD é percebida não como uma obrigação, mas como um benefício intrínseco ao *design* do sistema (LESCISIN; MAHMOUD, 2023).

Na seção seguinte, será explorado mais profundamente o tema de *Privacy by Design*, destacando como sua aplicação prática pode transformar tanto a conformidade regulatória quanto a essência do desenvolvimento seguro e ético de aplicativos móveis. Essa discussão é fundamental para entender como os princípios de privacidade e segurança podem ser

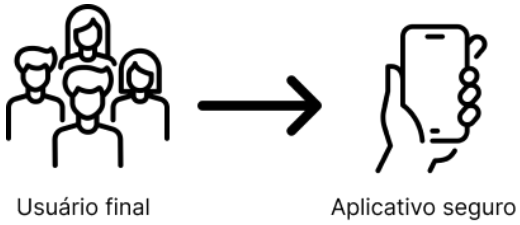
incorporados desde o início do processo de desenvolvimento, garantindo um ambiente digital mais seguro e confiável para todos os usuários.

4 Privacy by Design

A origem desta metodologia é apresentada em um depoimento da própria autora, que conforme seu relato surgiu em meados de 1990, enquanto atuava como Comissário de Informação e Privacidade de Ontário, Canadá, que percebeu que para salvaguardar a privacidade, a legislação e a regulamentação disponíveis já não seriam suficientes (CAVOUKIAN, 2012). Estabeleceu então, um paradigma fundamental no desenvolvimento de sistemas e aplicativos, enfatizando a importância da privacidade desde a concepção do projeto, baseando-se em sete princípios fundamentais (CAVOUKIAN et al., 2009). Esse enfoque é especialmente crucial em aplicações móveis na área da saúde, onde a manipulação segura de dados sensíveis é imprescindível. Ao integrar a privacidade no design e na operação de tecnologias e práticas de negócio desde o início, PbD garante não apenas a confiança dos usuários, mas também a conformidade com regulamentos rigorosos de proteção de dados, tais como a LGPD (LESCISIN; MAHMOUD, 2023).

A implementação dos princípios do PbD em aplicativos móveis de saúde demonstra um compromisso com a proteção proativa dos dados dos usuários, abordando potenciais ameaças à privacidade antes mesmo que elas se materializem, fazendo com que o usuário final esteja totalmente seguro e protegido mesmo que o mesmo não se preocupe em tomar cuidado com segurança, pois a implementação do PbD é a nível de desenvolvimento. Como exemplificado na Figura 1, o usuário final não tem acesso ao PbD diretamente, mas é proporcionalmente afetado pelo mesmo já que o contato direto com o aplicativo já o inclui em um ambiente seguro.

Figura 1 – Fluxo usuário aplicativo.



Fonte: Próprio autor

Abaixo são apresentados os sete princípios fundamentais do PbD e sua aplicação no desenvolvimento de aplicativos móveis na área da saúde (CAVOUKIAN et al., 2009):

1. **Proativo, não reativo; preventivo, não corretivo:** este princípio antecipa e neutraliza riscos à privacidade antes de sua concretização, reforçando a ideia de que a prevenção é preferível à correção. Diversos aplicativos de saúde disponíveis têm sido identificados na literatura (PIRES et al., 2020) e são utilizados por médicos e pacientes. Um vazamento de dados relacionado às informações de pacientes pode acarretar em situações jurídicas devido à exposição desses dados e até mesmo colocar a vida dos pacientes em risco.

2. **Privacidade como configuração padrão:** Garante a máxima proteção de privacidade sem exigir ação adicional por parte do usuário, fornecendo segurança desde o primeiro uso. A confiança na tecnologia pode ser um dos fatores que tem impactado no uso de recursos tecnológicos para a tomada de decisão médica (MORALES; OURIQUE; CAZELLA, 2021).

3. **Privacidade incorporada ao *design*:** A privacidade é considerada um componente essencial do desenvolvimento de aplicativos, não um adicional ou uma reflexão tardia. Conforme os artigos que exploraram as vulnerabilidades dos aplicativos (PRIAMBODO et al., 2022), se as aplicações em saúde incorporarem a privacidade na concepção do projeto, poderão ser ampliadas as possibilidades de uso para a área da saúde fornecendo ferramentas de apoio aos profissionais e pacientes mais confiáveis.

4. **Funcionalidade total – soma positiva, não soma zero:** PbD prova que é viável desenvolver sistemas que simultaneamente protegem a privacidade do usuário e fornecem funcionalidade completa. Ou seja, desenvolver aplicações com segurança não deve comprometer o resultado final do produto para a área da saúde.

5. **Segurança de ponta a ponta – proteção total dos dados:** Desde a coleta até a eliminação dos dados, todas as fases do processo garantem a segurança e a privacidade dos dados. Este pincípio, com certeza, é um dos mais relevantes para melhorar a confiança na tecnologia para a área da saúde. As soluções que tem sido propostas incorporam aquisição de dados através de vestíveis, em projetos públicos, estas questões de segurança tem sido pouco exploradas (ZHANG; SHAHRIAR; RIAD, 2020).

6. **Visibilidade e transparência – mantenha-o aberto:** Operações e práticas de privacidade devem ser transparentes e passíveis de verificação, assegurando a integridade do sistema. A área da saúde opera com dados sensíveis, o que pode expor pacientes a situações constrangedoras ou que prejudiquem o paciente, permitir que o aplicativo seja verificado quanto a garantia da privacidade é essencial (MANOEL, 2022).

7. **Respeito pela privacidade do usuário – Privacidade como padrão:** O respeito aos interesses do indivíduo é prioritário, que pode ser o médico, o paciente ou até um cuidador. Através do aumento de aplicações já mencionadas, e o apelo pelo uso da tecnologia para melhorar o cuidado das pessoas (PIRES et al., 2020), esta premissa deve estar presente e refletir seu resultado ao longo de todo o processo de criação e desenvolvimento de aplicações móveis para a saúde.

A aplicabilidade desses princípios no desenvolvimento de aplicativos móveis na área da saúde é crucial para mitigar riscos e fortalecer a confiança dos usuários. A etiquetagem de variáveis de dados com informações sobre requisitos de privacidade e a inclusão de verificações de privacidade nos métodos de *software* são exemplos práticos de como os princípios do PbD podem ser efetivamente implementados (LESCISIN; MAHMOUD, 2023).

A integração do PbD no ciclo de vida de desenvolvimento de aplicativos móveis enfatiza a importância de considerar a privacidade do usuário em todas as fases do processo. Essa abordagem não só cumpre com as exigências legais de privacidade, mas também estabelece uma relação de confiança duradoura com os usuários, valorizando a segurança e

a confidencialidade de suas informações pessoais. A adoção dos princípios do PbD permite criar aplicativos que protegem a privacidade dos usuários e, simultaneamente, satisfazem suas necessidades sem comprometer a funcionalidade ou a segurança, consolidando a base para um ambiente digital mais seguro e confiável. Lembrando que para as classes de aplicativos mencionadas em (PIRES et al., 2020), existem aqueles utilizados por profissionais de saúde (monitoramento e diagnóstico de pacientes, aplicativos de cuidados pessoais, aplicativos de saúde psicológica, aplicativos educacionais e aplicativos de redes sociais), pacientes (aplicativos de cuidados individuais, como: esportes, jogos e diagnóstico, aplicativos para verificar seus parâmetros fisiológicos como: batimentos cardíacos e calorias, aplicativos para entrar em contato com seu profissional de saúde, aplicativos educacionais de saúde e aplicativos de redes sociais). Além disso, existe ainda uma classe a mais de usuários, que seriam os cuidadores, seja de idosos ou de pacientes que necessitam acompanhamento.

4.1 Mitigação de vulnerabilidades através do PbD

A aplicação dos princípios do PbD pode ser uma estratégia eficaz na mitigação das vulnerabilidades identificadas em aplicativos móveis, especialmente aqueles usados no setor de saúde, como mencionadas na Subseção 3.1. Ao relacionar os princípios do PbD listados nessa seção com as vulnerabilidades citadas, pode-se obter uma relação quase que direta, como exemplificada na Tabela 2. Ao observar o quadro, pode-se perceber também que alguns dos princípios se repetem e/ou compartilham relação com mais de uma vulnerabilidade, tornando-se assim, um ótimo parâmetro a ser seguido desde a concepção do aplicativo.

Tabela 2 – Relação entre vulnerabilidades em aplicativos móveis e princípios de PbD

Vulnerabilidade	**Princípios de Privacy by Design Relacionados**
Uso de algoritmos de criptografia fracos	Segurança de ponta a ponta
Códigos rígidos sensíveis	Privacidade incorporada ao design, Proativo não reativo
Falhas de autenticação e autorização	Privacidade incorporada ao design, Proativo não reativo
Armazenamento inseguro de dados	Segurança de ponta a ponta
Comunicação insegura	Segurança de ponta a ponta
Falhas na autorização de usuários	Proativo não reativo, Privacidade como configuração padrão
Ataques de injeção de código	Privacidade incorporada ao design, Proativo não reativo
Gestão inadequada de sessões e cookies	Proativo não reativo, Privacidade como configuração padrão
Vulnerabilidades em componentes de terceiros	Privacidade incorporada ao design, Proativo não reativo
Configurações de segurança inadequadas	Privacidade incorporada ao design
Falhas na implementação de controle de acesso	Privacidade incorporada ao design, Proativo não reativo

Fonte: Próprio Autor

A integração dos princípios de PbD no desenvolvimento de aplicativos móveis enfatiza a importância de considerar a segurança e a privacidade em todas as fases do processo. Ao adotar esses princípios, desenvolvedores podem criar aplicativos que não apenas satisfazem as necessidades dos usuários, mas também protegem suas informações pessoais de forma eficaz e confiável, estabelecendo uma base sólida para um ambiente digital seguro.

4.2 Integração de Premissas de Segurança com Princípios do PbD

A integração eficaz das premissas de segurança, encontradas na Subseção 3.2, com os princípios do PbD listados nesse seção, representa uma abordagem estratégica fundamental para o desenvolvimento seguro de aplicativos móveis. A comparação entre essas premissas e os princípios do PbD, como apresentada na Tabela 3, ilustra como cada aspecto do PbD pode ajudar a garantir e reforçar as premissas de segurança essenciais em aplicações de saúde móvel.

Tabela 3 – Comparação entre premissas de segurança e princípios do PbD

Premissas de Segurança	**Princípios de Privacy by Design**
Confidencialidade	Privacidade como configuração padrão, Segurança de ponta a ponta
Integridade	Segurança de ponta a ponta, Privacidade incorporada ao design
Autenticação	Privacidade incorporada ao design, Proativo não reativo
Autorização	Privacidade incorporada ao design, Proativo não reativo
Disponibilidade	Segurança de ponta a ponta, Proativo não reativo
Não Repúdio	Visibilidade e transparência, Proativo não reativo

Fonte: Próprio Autor

A aplicação dos princípios de PbD pode ser facilitada com a implementação de um package ou *framework* para desenvolvedores, permitindo que eles criem aplicativos mais seguros de maneira mais eficiente e eficaz. Este enfoque proativo não só cumpre com as exigências legais de privacidade, mas também fortalece a confiança dos usuários, ao assegurar que a privacidade e a segurança são consideradas desde o início do desenvolvimento de aplicativos, garantindo tanto o cumprimento das premissas de segurança, listadas na Tabela 3, quanto mitigando as vulnerabilidades listadas na Tabela 2.

Na próxima seção, será explorado em mais detalhes como a implementação dos princípios de PbD pode ser operacionalizada em um *framework* de desenvolvimento, detalhando as técnicas e estratégias que desenvolvedores podem utilizar para integrar a privacidade e a segurança em suas aplicações de forma abrangente e sistemática.

5 Framework para a Proteção da Privacidade

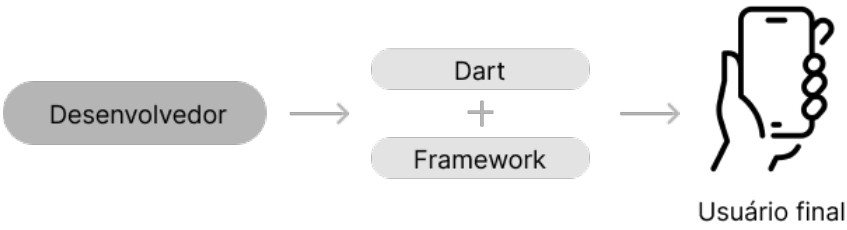
Conforme o estudo apresentado para o problema de privacidade dos dados, a implementação de um *framework* que utiliza *Privacy by Design* em Flutter[1] promove

[1] https://flutter.dev/

uma estratégia integrada, garantindo tanto a mitigação das vulnerabilidades, apresentadas nas seções anteriores, mais especificamente nas Tabelas 2 e 3, assegurando que todos os aspectos da privacidade e segurança sejam considerados desde a fase inicial de desenvolvimento. Diferente das soluções existentes que frequentemente focam em medidas reativas, a proposta atual sugere uma abordagem proativa, enfatizando a importância de incorporar a privacidade no design e desenvolvimento de aplicativos (MUNIM; ISLAM; ISLAM, 2019).

Este trabalho propõe o desenvolvimento de um *framework* em Flutter, designado a promover o PbD, que será útil tanto para plataformas Android quanto iOS. Este *framework* inovador emprega código nativo, desenvolvido em Kotlin[2] para Android e Swift[3] para iOS, para chamar métodos nativos que garantem a adesão aos princípios fundamentais de privacidade.

Figura 2 – Fluxo do framework.



Fonte: Próprio autor

O fluxo proposto neste trabalho envolve a criação e uso de um *package* em Flutter que permite ao desenvolvedor integrar facilmente as práticas do PbD, conforme ilustrado no fluxograma apresentado na Figura 2, o desenvolvedor utilizará o *package* diretamente com Dart, liguagem de programação para o *framework* Flutter, responsável por compilar aplicativos para iOS e Android. Esse código após compliado, transforma-se diretamente em um aplicativo que é disponibilizado ao consumidor final, oferecendo um nível superior de segurança e adequação às do PbD, garantindo uma experiência de usuário segura e confiável.

5.1 Implementação de Métodos Nativos para a Proteção da Privacidade

O *core* deste *framework* consiste na implementação de métodos nativos tanto em iOS, utilizando Swift, quanto em Android, utilizando Kotlin. Além de métodos nativos do próprio Flutter para fazer essa comunicação entre nativo e multiplataforma que se adequa e chama determinada função de forma correta de acordo com cada implementação feita, ou seja, uma mesma função chamada em Flutter vai ser executada corretamente no Android e no iOS de forma automática.

Com a implementação nativa feita e havendo uma comunicação limpa com o código em Flutter, qualquer desenvolvedor fica apto a entender e utilizar esse package em qualquer aplicativo, especificamente aplicativos na área da saúde, que tratam com muitos dados sensíveis de pacientes e de profissionais da saúde.

[2] https://kotlinlang.org/
[3] https://www.apple.com/br/swift/

Nessa seção será exemplificado como cada princípio do PbD foi implementado no package, junto com sua usabilidade e exemplos.

5.1.1 Proativo, não reativo; preventivo, não corretivo

A garantia fornecida por este princípio é fundamental no desenvolvimento, onde o *framework* implementado adota uma abordagem proativa na detecção de comportamentos anômalos ou suspeitos dos usuários. Utilizando métricas e eventos detalhados, que podem ser coletados através do *Firebase Analytics*, é possível monitorar ativamente padrões de interação dos usuários com o aplicativo.

Essas análises permitem identificar precocemente possíveis riscos de segurança, agindo antes que qualquer dano real possa ocorrer. Por exemplo, uma série de tentativas de login falhas ou atividades em horários incomuns pode acionar alertas que necessitam de atenção imediata.

Além do acompanhamento contínuo, é crucial estar sempre atento a possíveis problemas que possam surgir, garantindo que o aplicativo, mesmo em versões antigas, não apresente falhas. Para isso, o package oferece funcionalidades específicas para gerenciar dinamicamente o acesso dos usuários, como demonstrado nas seguintes funções implementadas no código do package:

```
SecurePrivacy.blockUser();
SecurePrivacy.unblockUser();
SecurePrivacy.isUserBlocked();
```

A função `blockUser()` é responsável por bloquear um usuário, utilizando métodos seguros para registrar este estado no sistema. A verificação do estado de bloqueio é feita através da função `isUserBlocked()`, enquanto a função `unblockUser()` permite remover o bloqueio. Estas funções devem ser utilizadas em conjunto com verificações de comportamento anômalo detectadas pelo sistema ou por uma análise manual do administrador do sistema, garantindo que ações preventivas sejam tomadas de forma eficaz.

Com as funções sendo chamadas corretamente, cabe ao desenvolvedor criar a lógica e telas para garantir o fluxo de bloqueio do usuário, fazendo com que o mesmo fique impossibilitado de acessar o aplicativo, como exemplificado na Figura 3. O que não necessariamente foi por erro do usuário, mas pode ser algum erro interno que possa prejudicar a segurança e assim evitando que ele se exponha ao problema.

Figura 3 – Usuário bloqueado.

Fonte: Próprio autor

A integração dessas funções com requisições ao servidor permite uma abordagem reativa baseada no contexto atual e nos dados analisados. Desta forma, permite que o bloqueio ou desbloqueio de usuários, seja uma resposta diretamente proporcional aos riscos identificados, mantendo o sistema seguro e respeitando os princípios de privacidade desde a concepção do projeto.

5.1.2 Privacidade como configuração padrão

A prevenção de capturas de tela é uma medida de segurança essencial no contexto do PbD. Especialmente, quando se trata de aplicativos que lidam com informações sensíveis, como dados de login ou informações pessoais de saúde. Este procedimento está diretamente alinhado com o princípio de privacidade como configuração padrão, garantindo que, por padrão, as informações pessoais dos usuários sejam protegidas contra exposição não autorizada.

Para facilitar a implementação desta funcionalidade em aplicativos desenvolvidos com os recursos propostos, os desenvolvedores podem ativar a proteção contra capturas de tela com comandos simples. Ao utilizar o comando:

```
SecurePrivacy.preventScreenshotOn();
```

O sistema é configurado para automaticamente impedir que capturas de tela sejam realizadas. Essa proteção pode ser desativada a qualquer momento com o comando:

```
SecurePrivacy.preventScreenshotOff();
```

No nível do código nativo, a implementação é adaptada para cada plataforma. Para dispositivos Android, é utilizado Kotlin para ajustar as configurações de segurança da janela da atividade com o seguinte trecho de código:

```
val window = activity?.window
window?.setFlags(
  android.view.WindowManager.LayoutParams.FLAG_SECURE,
  android.view.WindowManager.LayoutParams.FLAG_SECURE
)
```

Para dispositivos iOS, o Swift é empregado para ativar a proteção contra capturas de tela através do *ScreenProtectorKit*, ilustrado abaixo:

```
enabledPreventScreenshot = .on
screenProtectorKit?.enabledPreventScreenshot()
```

Essas medidas garantem que informações críticas sejam protegidas de capturas de tela indevidas e não autorizadas, reforçando a segurança e a confiança no uso de aplicativos desenvolvidos com este *framework*. A Figura 4 ilustra o resultado com o uso da funcionalidade.

Essas prevenções vão forçar um usuário não preocupado com a segurança a se manter dentro do ambiente seguro ao garantir que ele não consiga tirar prints de algumas

Figura 4 – Proteção contra capturas de tela desativada e ativada.

Fonte: Próprio autor

telas, ou de todas, dependendo da configuração escolhida pelo desenvolvedor, sejam em telas de login ou telas com dados sensíveis de pacientes, como por exemplificado na Figura 4. Essa prevenção vai fazer com que ao tirar uma screenshot, o retorno da imagem nunca seja os dados sensíveis, mas sim uma imagem totalmente preta.

5.1.3 Privacidade incorporada ao design

A incorporação da privacidade no design do *framework* é um dos pilares fundamentais para garantir que todos os aspectos da proteção de dados sejam considerados desde o início do desenvolvimento de um aplicativo. Este princípio assegura que as medidas de privacidade não sejam apenas adições posteriores, mas sim partes integrantes do processo de desenvolvimento de *software*.

Para implementar essa funcionalidade no package proposto, várias técnicas e estratégias são empregadas desde as fases iniciais do design. Uma dessas estratégias é a inclusão de componentes de *software* que automaticamente gerenciam os dados de acordo com as normativas de privacidade vigentes, como a LGPD, que pode ser alcançada dessa forma:

```
SecurePrivacy.initializePrivacySettings();
```

Este comando configura o ambiente de desenvolvimento para aderir automaticamente às melhores práticas de privacidade, garantindo que todos os módulos do aplicativo tratem os dados de forma segura e conforme os regulamentos.

No nível do código do package, ele define que será utilizado essas diretrizes implementadas diretamente na gestão do package em si durante o uso do aplicativo. Por padrão, essa função ira ser ativada automaticamente ao utilizar o package, podendo ser desativada conforme necessidade do desenvolvedor utilizando a função:

```
SecurePrivacy.stopPrivacySettings();
```

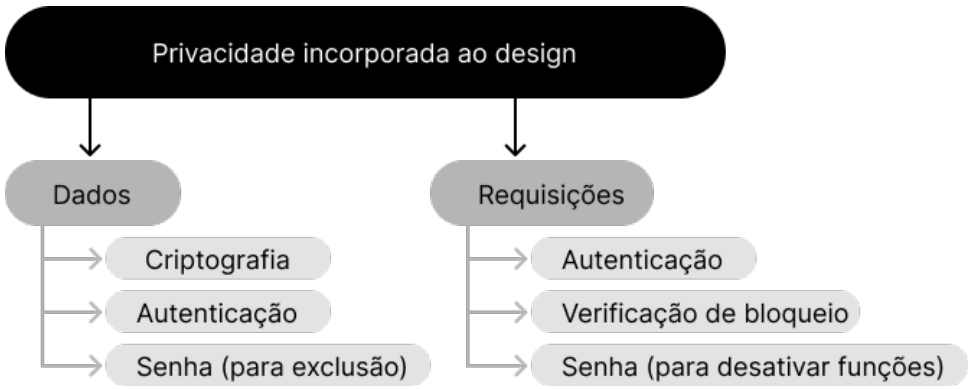
E para garantir um bom fluxo no desenvolvimento, é possível verificar se essa função está ativa atravez do código abaixo que retorna um boolean:

```
SecurePrivacy.isPrivacySettingsActived();
```

Ao manter a função ativa, o package proposto irá gerenciar de forma automática os requisitos de seguranças para garantir que a aplicação funcione de forma segura, tais como automaticamente criptografar todas as informações antes de salvar no banco de dados do próprio dispositivo e controlar a autênticidade do usuário, fazendo requisições de token de autenticação para quaisquer tipo de solicitação ao package.

Essas medidas garantem que o design e desenvolvimento do aplicativo estejam alinhados com os princípios de privacidade desde o início, promovendo uma base sólida de confiança e segurança para os usuários finais. Além disso, essas configurações permitem que os desenvolvedores se concentrem mais nas funcionalidades do aplicativo, deixando que o *framework* cuide dos aspectos relacionados à privacidade.

Figura 5 – Integração da privacidade no design do aplicativo.



Fonte: Próprio autor

O fluxograma presente na Figura 5 exemplifica como a privacidade é integrada no package proposto, garantindo que as funcionalidades passem por uma camada extra de segurança de forma nativa, sendo requisitado informações extras para garantir a autenticiadde de requisições e de acesso aos dados. Sendo assim necessário a verificação do token do usuário toda vez que alguma requisição do package ou acesso ao banco de dados é feita e em alguns casos um pedido de senha, que pode ser diretamente integrada com uma API externa de necessidade do desenvolvedor para verificação da senha e retornar a validação caso a senha esteja correta.

5.1.4 Funcionalidade Total – soma positiva, não soma zero

Este princípio está intrinsecamente ligado à maneira como as funcionalidades são implementadas em relação aos outros princípios do PbD, especialmente no que tange a integração com APIs externas e a comunicação com servidores próprios. A ideia central é que a aplicação deve manter uma funcionalidade completa sem comprometer a privacidade e segurança dos dados.

Ao integrar serviços externos por meio de APIs, é crucial que o package proposto gerencie essas conexões de forma que preserve a integridade e a confidencialidade dos dados. Isso significa que todas as interações com servidores externos devem ser projetadas para garantir que as medidas de segurança e privacidade sejam mantidas em todos os níveis de comunicação.

O desenvolvimento e uso de servidores próprios deve também respeitar os princípios do PbD, assegurando que o tratamento dos dados coletados, processados e armazenados seja feito de forma a proteger a privacidade do usuário desde a concepção do sistema. O package se propõe a oferecer mecanismos que assegurem o uso correto das APIs e a proteção adequada ao acessar serviços externos, garantindo que a funcionalidade e a privacidade sejam alcançadas simultaneamente.

Para a funcionalidade do package, ele possui a função:

```
SecurePrivacy.validateServerCommunication(String url);
```

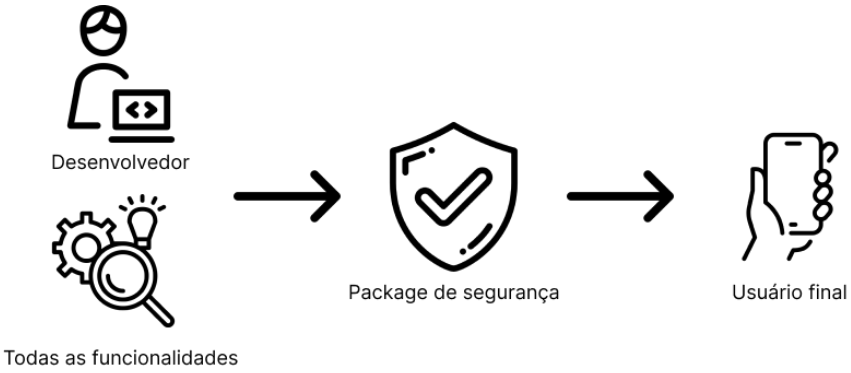
Que visa consultar e verificar se a url da API a qual se deseja conectar possui algum risco e se é totalmente segura para troca de dados entre cliente servidor.

Para gerência de requisições na API, foi proposto uma chamada na função:

```
final apiService =  SecurePrivacy.ApiService();
```

Que instancia o ApiService() que funciona basicamente como um http request onde pode-se fazer requisições de GET, POST e PATCH, ficando vetado toda a chamada para DELETE para uma verificação extra de senha caso definido o padrão de segurança explicado na Subseção 5.1.3.

Figura 6 – Todas funcionalidades disponíveis.



Fonte: Próprio autor

Estas funções do package proposto ajudam a garantir que as comunicações e integrações externas estejam alinhadas com as políticas de privacidade estabelecidas, como exemplificado na Figura 6, onde o desenvolvedor abstrai todas as funcionalidades necessárias para o funcionamento do sistema para utilização do package proposto, promovendo um ambiente de aplicação seguro e confiável.

5.1.5 Segurança de ponta a ponta – proteção total dos dados

Este princípio do PbD garante a segurança dos dados desde o início até o fim do seu ciclo de vida, abrangendo desde o momento em que são coletados até sua eliminação, onde a segurança não deve ser tratada apenas em pontos isolados, mas sim integrada

de maneira contínua e completa em todas as etapas do tratamento de dados dentro do aplicativo.

A aplicação deste princípio começa já na interface do usuário, onde, conforme abordado anteriormente na Subseção 5.1.2 sobre Privacidade como configuração padrão, medidas como prevenção de captura de tela garantem que dados sensíveis não sejam expostos indevidamente. Isso estabelece a primeira camada de proteção, assegurando que mesmo as interações mais básicas com o aplicativo sejam seguras.

Além disso, o tratamento dos dados dentro do sistema é rigorosamente controlado. Uma das principais ferramentas empregadas é a criptografia, que é aplicada automaticamente a todos os dados armazenados pelo aplicativo. Utilizando o comando:

```
SecurePrivacy.saveData(seu_dado_id,seu_dado);
```

Qualquer dado inserido pelo usuário é imediatamente criptografado antes de ser salvo no dispositivo. Esta criptografia não é uma operação isolada; ela faz parte de uma camada de segurança que inclui criptografia adicional para garantir que, mesmo durante o processo de descriptografia, os dados permaneçam protegidos e inacessíveis a agentes não autorizados.

Figura 7 – Fluxograma de criptografia de dados.

Fonte: Próprio autor

No nível do código nativo, a implementação varia conforme a plataforma. Para dispositivos iOS, utiliza-se o sistema Keychain para gerenciar o armazenamento seguro das informações:

```
let keychainItem = KeychainItem(service: "com.example.yourapp", account: "user")
try keychainItem.savePassword("senha_segura")
```

Em dispositivos Android, é adotada a criptografia AES, complementada com uma chave RSA armazenada seguramente no KeyStore:

```
val encryptedData = encryptAES(data, aesKey)
val encryptedKey = encryptRSA(aesKey, publicKey)
saveToKeystore(encryptedKey, encryptedData)
```

Estas medidas garantem que a segurança dos dados seja mantida não apenas em sua armazenagem, mas também durante a transferência entre o cliente e o servidor, como ilustrado na Figura 7. Este fluxograma mostra o processo pelo qual os dados do

usuário, ao serem transferidos para o aplicativo, são criptografados antes de atingirem o armazenamento local. E por fim há a função:

```
SecurePrivacy.deleteData(seu_dado_id, password);
```

que é responsável pela remoção do seu dado do dispositivo de maneira definitiva, passando assim o id do dado salvo e ocasionalmente a senha de segurança, caso definido o padrão de design explicado na Subseção 5.1.3.

5.1.6 Visibilidade e transparência – mantenha-o aberto

Este princípio é um dos mais críticos dentro do PbD, pois é o que mais se aproxima do usuário final, concedendo-lhe poder substancial sobre seus próprios dados, onde a visibilidade e transparência não só fortalecem sua confiança, mas também o assegura que esteja plenamente informado sobre quais dados são coletados e armazenados pela aplicação.

Uma funcionalidade chave do *framework* proposto para apoiar este princípio é a:

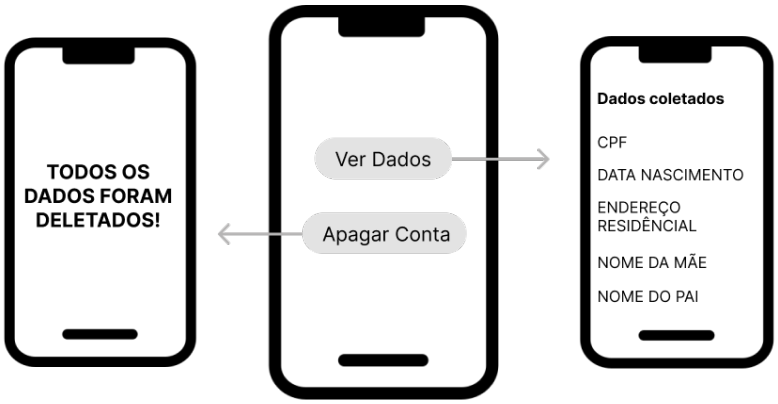
```
SecurePrivacy.getAllDataSaved();
```

Ao invocar esta função, o usuário não recebe diretamente os dados, mas sim uma descrição dos parâmetros que foram salvos, tais como nome e CPF. Essa abordagem garante que o usuário esteja ciente dos dados coletados sem comprometer a segurança ou exibir os dados sensíveis diretamente. A exibição dessas informações é pré-definida pelo desenvolvedor, mas deve obrigatoriamente listar todos os dados coletados.

Adicionalmente, é providenciado um mecanismo para que os usuários possam apagar completamente suas contas e todos os dados associados de forma segura e irreversível. Isso é facilitado pela função:

```
SecurePrivacy.deleteAllData();
```

Figura 8 – Controle do usuário sobre seus dados.



Fonte: Próprio autor

A Figura 8 ilustra a interface do aplicativo onde o usuário pode visualizar seus dados ou optar por excluí-los. Existem dois botões principais: um para ver dados, que

aciona o fluxo para exibir os parâmetros de dados salvos, e outro para apagar conta, que inicia o processo de exclusão de dados após a confirmação por e-mail. Esta função garante que o usuário tenha controle total e transparente sobre suas informações pessoais, alinhando-se totalmente com o princípio de visibilidade e transparência.

5.1.7 Respeito pela privacidade do usuário – Privacidade como padrão

Este princípio do PbD enfatiza a importância de configurar o sistema para maximizar a privacidade do usuário desde o início, sem a necessidade de intervenção manual para proteger seus dados. Fundamentalmente, é vital criar um ambiente em que o usuário possa facilmente gerenciar as configurações de privacidade, permitindo ou não a coleta de dados conforme sua preferência, enquanto ainda se respeita a necessidade de coletar dados mínimos necessários para o funcionamento do aplicativo, como discutido na Subseção 5.1.4.

Como observado na Figura 9, basicamente esse método consiste em dar ao usuário liberdade para escolher quais dados podem ser coletados, mas sem prejudicar o sistema, ou seja, não poderá desativar os dados que são essenciais para o aplicativo funcionar de maneira correta.

Figura 9 – Configuração de privacidade do usuário.

Fonte: Próprio autor

A implementação desse ambiente é facilitada por duas funções principais do *framework* proposto:

```
SecurePrivacy.getUserSettings();
```

Esta função retorna um Map<String, Boolean> que indica quais dados o usuário optou por permitir que o aplicativo colete. Por exemplo, o retorno pode ser algo como:

```
{"name": true, "age": true, "cpf": false}
```

indicando que o usuário permite a coleta de seu nome e idade, mas não do seu CPF. E para modificar essas configurações, o usuário pode utilizar a função:

```
SecurePrivacy.setUserSettings(Map<String, bool> preferences);
```

que permite ao usuário atualizar suas preferências de privacidade de forma simples e segura, semelhante à maneira como os sites solicitam consentimento para cookies.

A Figura 9 mostra uma interface típica de configurações de privacidade dentro do aplicativo, onde o usuário pode escolher quais informações ele permite que sejam coletadas. Esse exemplo ilustra configurações para nome, idade e CPF, refletindo as preferências do usuário conforme mostrado no exemplo de configuração.

Essa abordagem assegura que o usuário tenha controle total sobre seus dados pessoais, fortalecendo sua confiança no aplicativo ao garantir que suas preferências de privacidade sejam respeitadas e facilmente gerenciáveis.

5.2 Importância da Implementação:

A integração dessas medidas de segurança não apenas fortalece a proteção de dados pessoais, mas também assegura que o aplicativo esteja em conformidade com as normativas de privacidade. Ao facilitar a adoção de práticas de segurança robustas, o *framework* proposto contribui significativamente para a confiança e segurança do usuário, pilares essenciais para o sucesso de aplicativos móveis na era digital.

A introdução deste *framework* em Flutter para a incorporação de práticas de privacidade oferece múltiplos benefícios, incluindo:

- **Facilidade de Integração:** Permite aos desenvolvedores implementar medidas de proteção de privacidade complexas com simplicidade, por meio de chamadas de métodos pré-definidos.
- **Universalidade:** Oferece soluções compatíveis com as principais plataformas móveis, garantindo a uniformidade na proteção de privacidade em diferentes dispositivos.
- **Conformidade com Princípios de Privacidade:** Assegura que os aplicativos desenvolvidos com o *framework* estejam alinhados com os princípios do PbD, reforçando a segurança dos dados do usuário desde a concepção.

O desenvolvimento deste *framework* representa um passo importante para a integração da privacidade nas fases iniciais do design de aplicativos móveis. Ao facilitar a implementação de práticas de proteção de privacidade, este *framework* busca não apenas cumprir com as regulamentações atuais, mas também promover uma mudança significativa na maneira como a privacidade é percebida e gerenciada no desenvolvimento de *software*.

6 Conclusão

Este trabalho abordou a segurança e privacidade em aplicativos móveis, com um foco especial na área da saúde, um setor que tem visto uma rápida expansão e digitalização. O objetivo do trabalho foi bem sucedido apresentando um *framework*, em Flutter baseado em princípios de *Privacy by Design*, demonstrando-se uma estratégia interessante para os desenvolvedores de aplicativos móveis. Desta forma é possível incorporar segurança e privacidade de dados desde a concepção do desenvolvimento da aplicação, alinhando-se às exigências da legislação vigente; e destacando, a importância de construir aplicativos que protegem os usuários da área da saúde, nos quais destaca-se, profissionais de saúde, pacientes e cuidadores.

Como demonstrado em (ALIASGARI; BLACK; YADAV, 2018), aplicativos móveis possuem várias vulnerabilidades, revelou uma série de desafios, como falhas de segurança da rede, autenticação inadequada e ataques *Man-in-the-Middle*, que são significativamente amplificados no contexto da saúde devido à sensibilidade dos dados tratados. A aplicação de práticas recomendadas sobre mecanismos de segurança, incluindo a implementação de criptografia forte e métodos de autenticação robustos, provou ser crucial para mitigar esses riscos (PIRES et al., 2020).

Além disso, a pesquisa destacou a relevância do *Privacy by Design*, que foi explorado através do desenvolvimento de métodos nativos como prevenção capturas de tela e criptografia de dados, garantindo que as aplicações móveis atendam não apenas às necessidades técnicas de segurança, mas também às normativas legais e éticas de privacidade (LESCISIN; MAHMOUD, 2023). A funcionalidade de prevenção de captura de tela, em particular, demonstra uma aplicação prática dos princípios de privacidade desde o design, proporcionando uma camada adicional de segurança que protege as informações sensíveis dos usuários contra exposição não autorizada.

Este estudo também contribui para a literatura ao fornecer lacunas sobre como as abordagens de desenvolvimento podem ser melhoradas para integrar a segurança e privacidade de maneira mais efetiva. Através deste trabalho, reforça-se a ideia de que a proteção dos dados do usuário deve ser uma prioridade contínua, impulsionando a adoção de uma cultura de segurança que vai além do cumprimento de requisitos regulatórios.

Em conclusão, a implementação deste *framework* em Flutter é um passo fundamental para promover um ambiente digital mais seguro e confiável para aplicativos móveis, especialmente na área da saúde. A pesquisa sublinha a importância de uma abordagem holística na proteção de dados, que é vital não só para a conformidade regulatória, mas também para a manutenção da confiança dos usuários na era digital.

Referências

ALIASGARI, M.; BLACK, M.; YADAV, N. Security vulnerabilities in mobile health applications. In: *2018 IEEE Conference on Application, Information and Network Security (AINS)*. [S.l.: s.n.], 2018. p. 21–26. Citado (4) vezes nas páginas [6, 8, 9 e 26].

ANIKEEV, M.; SHULMAN, H.; SIMO, H. Privacy policies of mobile apps - a usability study. In: *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. [S.l.: s.n.], 2021. p. 1–2. Citado na página [8].

CAVOUKIAN, A. Privacy by design [leading edge]. *IEEE Technology and Society Magazine*, IEEE, v. 31, n. 4, p. 18–19, 2012. Citado na página [12].

CAVOUKIAN, A. et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, v. 5, p. 12, 2009. Citado (2) vezes nas páginas [6 e 12].

GARDNER, J. et al. Helping mobile application developers create accurate privacy labels. In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*. [S.l.: s.n.], 2022. p. 212–230. Citado na página [8].

GUDLUR, T. D. V. V. R. Fintech future business cyber vulnerabilities and challenges. In: *2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)*. [S.l.: s.n.], 2023. p. 1–4. Citado (3) vezes nas páginas [6, 8 e 11].

KEINERT, T. M. M.; CORTIZO, C. T. Dimensões da privacidade das informações em saúde. *Cadernos de Saúde Pública*, Escola Nacional de Saúde Pública Sergio Arouca, Fundação Oswaldo Cruz, v. 34, n. 7, p. e00039417, 2018. ISSN 0102-311X. Disponível em: <https://doi.org/10.1590/0102-311X00039417>. Citado (2) vezes nas páginas [6 e 7].

LESCISIN, M.; MAHMOUD, Q. H. Design and development of policy enforcement for the privacy by design framework. In: *2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*. [S.l.: s.n.], 2023. p. 1–6. Citado (5) vezes nas páginas [6, 11, 12, 13 e 26].

LI, N.; YE, Q. Mobile data collection and analysis with local differential privacy. In: *2019 20th IEEE International Conference on Mobile Data Management (MDM)*. [S.l.: s.n.], 2019. p. 4–7. Citado (2) vezes nas páginas [7 e 8].

MANOEL, B. de E. *Análise da Viabilidade de Uma Camada de Segurança para um Dispositivo Vestível Cardíaco Empregando Conceitos de Internet das Coisas Médicas*. 2022. Citado (2) vezes nas páginas [10 e 13].

MHLANGA, M. X.; MAITI, R. R.; HAMMER, B. Privacy and security matters related to use of mobile devices and social media. In: *SoutheastCon 2021*. [S.l.: s.n.], 2021. p. 1–6. Citado na página [8].

MORALES, A. S.; OURIQUE, F. d. O.; CAZELLA, S. C. A comprehensive review on the challenges for intelligent systems related with internet of things for medical decision. *Enhanced telemedicine and e-health: advanced IoT enabled soft computing framework*, Springer, p. 221–240, 2021. Citado na página [13].

MUNIM, K. M.; ISLAM, I.; ISLAM, M. N. A conceptual framework for improving privacy in mobile operating systems. In: *2019 2nd International Conference on Innovation in Engineering and Technology (ICIET)*. [S.l.: s.n.], 2019. p. 1–6. Citado na página [16].

PIRES, I. M. et al. A research on the classification and applicability of the mobile health applications. *Journal of Personalized Medicine*, v. 10, n. 1, p. 11, 2020. Disponível em: <https://doi.org/10.3390/jpm10010011>. Citado (5) vezes nas páginas [6, 12, 13, 14 e 26].

PRIAMBODO, D. F. et al. Mobile health application security assesment based on owasp top 10 mobile vulnerabilities. In: *2022 International Conference on Information Technology Systems and Innovation (ICITSI)*. [S.l.: s.n.], 2022. p. 25–29. Citado (4) vezes nas páginas [8, 9, 11 e 13].

WIERINGA, J. et al. Data analytics in a privacy-concerned world. *Journal of Business Research*, v. 122, p. 915–925, 2021. ISSN 0148-2963. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0148296319303078>. Citado (2) vezes nas páginas [7 e 8].

XIONG, J. et al. A personalized privacy protection framework for mobile crowdsensing in iiot. *IEEE Transactions on Industrial Informatics*, v. 16, n. 6, p. 4231–4241, 2020. Citado (2) vezes nas páginas [7 e 11].

YAQUB, M. et al. Privacy policies of free medical, health, fitness mobile applications and the gdpr. In: *2023 5th International Conference on Intelligent Medicine and Image Processing (IMIP)*. [S.l.: s.n.], 2023. p. 84–96. Citado (2) vezes nas páginas [7 e 8].

ZANON, V. et al. Avaliação experimental de uma camada de segurança implementada em dispositivo vestível cardíaco para internet das coisas médicas. In: *Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Porto Alegre, RS, Brasil: SBC, 2022. p. 97–110. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbseg/article/view/21661>. Citado (2) vezes nas páginas [6 e 10].

ZHANG, C.; SHAHRIAR, H.; RIAD, A. B. M. K. Security and privacy analysis of wearable health device. In: *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. [S.l.: s.n.], 2020. p. 1767–1772. Citado (2) vezes nas páginas [8 e 13].

ZHOU, W. et al. Reviewing iot security via logic bugs in iot platforms and systems. *IEEE Internet of Things Journal*, v. 8, n. 14, p. 11621–11639, 2021. Citado na página [11].