UNIVERSIDADE FEDERAL DO CEARÁ

INSTITUTO UNIVERSIDADE VIRTUAL

CURSO DE GRADUAÇÃO EM SISTEMAS E MÍDIAS DIGITAIS

RÔMULO EVANGELISTA FERREIRA

UM ESTUDO EXPLORATÓRIO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DAS VULNERABILIDADES EM *SMARTPHONES* ANDROID

FORTALEZA

2022

RÔMULO EVANGELISTA FERREIRA

UM ESTUDO EXPLORATÓRIO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DAS VULNERABILIDADES EM *SMARTPHONES* ANDROID

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas e Mídias Digitais do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas e Mídias Digitais.

Orientador: Prof. Dr. Leonardo Oliveira Moreira

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

F443e Ferreira, Rômulo Evangelista.
Um Estudo Exploratório sobre a Lei Geral de Proteção de Dados Pessoais na Perspectiva das Vulnerabilidades em Smartphones Android / Rômulo Evangelista Ferreira. – 2022.
44 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Instituto UFC Virtual, Curso de Sistemas e Mídias Digitais, Fortaleza, 2022.
Orientação: Prof. Dr. Leonardo Oliveira Moreira.

1. Lei Geral de Proteção de Dados Pessoais. 2. Vulnerabilidades. 3. Android. I. Título.

CDD 302.23

RÔMULO EVANGELISTA FERREIRA

UM ESTUDO EXPLORATÓRIO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DAS VULNERABILIDADES EM *SMARTPHONES* ANDROID

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas e Mídias Digitais do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas e Mídias Digitais.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Leonardo Oliveira Moreira (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Gilvan Rodrigues Maia
Universidade Federal do Ceará (UFC)

Prof. Dr. Ernesto Trajano de Lima Neto
Universidade Federal do Ceará (UFC)

À minha família, especialmente à minha mãe, Maria Simone Silva e meu pai, Ramiro Paulo de Lima Conceição, que sempre acreditaram e investiram na minha educação e de meu irmão. O apoio e exemplo que vocês me deram sempre me manteve firme nessa caminhada.

AGRADECIMENTOS

Aos meus pais por sempre apoiar e incentivar os estudos, por todo investimento na minha educação e do meu irmão. Entender que o conhecimento liberta e abre portas foi de extrema importância para minha vida. O exemplo que foi passado por vocês, sempre será minha base.

À toda minha família por sempre torcerem e incentivarem na minha caminhada. Especialmente ao meu irmão, Álvaro e meu tio, Nonato, por sempre estarem disponíveis para vencer os obstáculos enfrentados durante a graduação.

À minha namorada, Carolini Nascimento, que sempre me apoiou e me motivou a continuar em frente, mesmo diante das dificuldades.

Aos meus amigos pelo apoio durante toda minha graduação. Aos que se formaram antes de mim, pude acompanhar e sentir a felicidade por atingir esse objetivo tão desejado. Aos que ainda estão cursando, continuarei apoiando e aguardando para compartilhar este sentimento com vocês.

Ao Prof. Dr. Leonardo Oliveira Moreira por me orientar em meu trabalho de conclusão de curso.

À todos os professores do curso que foram os responsáveis por formar a base de conhecimento que aplico e aplicarei na vida.

Ao Doutorando em Engenharia Elétrica, Ednardo Moreira Rodrigues, e seu assistente, Alan Batista de Oliveira, aluno de graduação em Engenharia Elétrica, pela adequação do *template* utilizado neste trabalho para que o mesmo ficasse de acordo com as normas da biblioteca da Universidade Federal do Ceará (UFC).

À Universidade Federal do Ceará por proporcionar um ensino de qualidade com estrutura adequada para minha formação.

"We are the champions, my friends. And we'll keep on fighting till the end."

(Queen)

RESUMO

No Brasil, segundo um estudo da Fundação Getúlio Vargas em 2020, cada habitante tinha cerca de 2 dispositivos digitais, um total de 440 milhões de dispositivos. O aumento da conectividade e a popularização da Internet, possibilitaram o cidadão realizar quase todas as suas tarefas habituais de forma conectada como: realizar transações bancárias, compras on-line, agendar atendimentos, conectar-se com amigos, etc. Portanto, tais dispositivos armazenam uma quantidade significativa de dados sensíveis, além de documentos e fotos pessoais. Alguns destes dados são armazenados em nuvens ou no próprio aparelho, mas o usuário não tem o controle sobre como eles são manipulados e acessados. Sendo assim, os usuários de *smartphones* necessitam de recursos que protejam seus dados tanto no nível de leis quanto no uso de técnicas computacionais. Como forma de transparecer e responder como estes dados vêm sendo utilizados, existe a Lei Geral de Proteção de Dados Pessoais (LGPD) que regula as atividades de tratamento de dados pessoais. Este trabalho tem como objetivo apresentar uma avaliação sobre o impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) em aplicações móveis na intenção de mitigar ou eliminar possíveis vulnerabilidades de dados. Como resultados, foi apresentado um protótipo de aplicativo Android para analisar as vulnerabilidades em sistemas Android e como a LGPD poderia mitigar estas vulnerabilidades.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais. Vulnerabilidades. Android.

ABSTRACT

In Brazil, according to a study by the Getúlio Vargas Foundation in 2020, each inhabitant had about 2 digital devices, a total of 440 million devices. The increase in connectivity and the popularization of the Internet have enabled citizens to carry out almost all of their usual tasks online, such as: performing bank transactions, online shopping, scheduling appointments, connecting with friends, etc. Therefore, such devices store a significant amount of sensitive data, in addition to personal documents and photos. Some of this data is stored in clouds or on the device itself, but the user does not have control over how they are manipulated and accessed. Therefore, smartphone users need resources that protect their data both in terms of laws and in the use of computational techniques. As a way to show and respond to how this data is being used, there is the General Law for the Protection of Personal Data (LGPD) that regulates the activities of processing personal data. This work aims to present an assessment of the impact of the General Law for the Protection of Personal Data (LGPD) on mobile applications with the intention of mitigating or eliminating possible data vulnerabilities. As a result, an Android application prototype was presented to analyze vulnerabilities in Android systems and how the LGPD could mitigate these vulnerabilities.

Keywords: General Personal Data Protection Law. Vulnerabilities. Android.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interface*
ASCII	*American Standard Code for Information Interchange*
CPF	Cadastro de Pessoas Físicas
EU	União Europeia
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
RG	Registro Geral
SSL	*Secure Sockets Layer*
TI	Tecnologia da Informação
TLS	*Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO

No Brasil, segundo um estudo da Fundação Getúlio Vargas (FGV) - 32ª Edição, 2020 (MEIRELLES, 2020), cada habitante tinha cerca de 2 dispositivos digitais (computadores, *notebooks*, *tablets* e *smartphones*), um total de 440 milhões de dispositivos. Além disso, o Brasil foi o décimo país em que a Internet mais cresceu, houve um aumento de 7,2%, o que representa quase dez milhões de pessoas; já entre os anos de 2019 e 2020, o número de usuários cresceu 6%, ou seja, 8,5 milhões de pessoas adquiriram o direito de acesso à rede mundial de computadores (BAGATINI *et al.*, 2021). Segundo Kemp (2020), a penetração da Internet em solo brasileiro é de 71% da população total do país.

O aumento da conectividade e a popularização da Internet, possibilitaram o cidadão realizar quase todas as suas tarefas habituais de forma conectada como: realizar transações bancárias, compras *on-line*, agendar atendimentos, conectar-se com amigos, etc. Com a disseminação e popularização dos *smartphones* aumentou ainda mais essa conectividade dos cidadãos com a Internet (BAGATINI *et al.*, 2021). Os *smartphones* chamam a atenção pela sua mobilidade e poder computacional próximos aos computadores. Estes dispositivos permitem a instalação de aplicativos de bancos, redes sociais e muitos serviços para interagir com seus clientes. Portanto, tais dispositivos armazenam uma quantidade significativa de dados sensíveis, além de documentos e fotos pessoais. Alguns destes dados são armazenados em nuvens ou no próprio aparelho, mas o usuário não tem o controle sobre como eles são manipulados e acessados. Sendo assim, os usuários de *smartphones* necessitam de recursos que protejam seus dados tanto no nível de leis quanto no uso de técnicas computacionais.

Como forma de transparecer e responder como estes dados vêm sendo utilizados, existe a Lei Geral de Proteção de Dados Pessoais (LGPD) que regula as atividades de tratamento de dados pessoais. A LGPD foi criada em agosto de 2018 e sancionada em setembro de 2020 (FARIAS; BARROS, 2022). Com a LGPD, empresas de diversos setores e tamanhos passaram a se preocupar em entender os impactos dessa nova lei em seus negócios. Desde então, empresas de segurança, escritórios de advocacias, profissionais da área de Tecnologia da Informação (TI), jurídico, entre outros profissionais, têm direcionado esforços para entender as novas exigências legais e ao mesmo tempo administrando os impactos diretos que isso representa para seus negócios (FARIAS; BARROS, 2022).

Uma corrida vem sendo travada para adequação à LGPD, seja para criação de novos sistemas ou manutenção de sistemas legado. Por isso, o objetivo principal deste trabalho é

auxiliar no desenvolvimento de aplicações para *smartphones* Android na adequação à LGPD.

1.1 Motivação

Estando no mercado de trabalho, foi possível perceber um movimento relativamente preocupado com a adequação à LGPD. O momento em que a LGPD entrou em vigor, coincidiu com o cenário pandêmico do COVID-19.

Além de grandes e pequenas organizações estarem preocupadas com a adequação com a LGPD, era preciso, também, uma preocupação com os casos crescentes de COVID-19 em todo o mundo. Como já é sabido, a pandemia trouxe diversos impactos nos mais diversos setores. Economia foi um setor bastante atingido pelo contexto pandêmico.

O uso de aplicações móveis e *sites* para a *internet* aumentou consideravelmente durante a pandemia (Cetic.br, 2021). Isso se dá pelo fato das pessoas estarem em suas casas, aumentando o uso da *internet*. Muitos serviços foram migrados para permitir o acesso online.

Com isso, a LGPD impactou diretamente os aplicativos e *sites* no Brasil. Diversas empresas tiveram que se adaptar para que a LGPD fosse respeitada. Este movimento foi visto como bastante resiliente, uma vez que muitos serviços operaram normalmente e ganharam força no mercado.

1.2 Objetivos

O objetivo geral deste trabalho é apresentar uma avaliação sobre o impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) em aplicações móveis na intenção de mitigar ou eliminar possíveis vulnerabilidades de dados. Para atingir o objetivo geral, alguns objetivos específicos foram elencados:

a) estudar a LGPD e os aspectos de desenvolvimento de aplicações móveis;
b) verificar os aspectos da LGPD que podem ser adotados em aplicações móveis; e
c) discutir como a LGPD pode aumentar a privacidade e proteção de dados pessoais em aplicações móveis por meio de provas de conceito.

1.3 Estrutura do Documento

O restante deste documento está organizado em cinco capítulos. O Capítulo 2 apresenta todo arcabouço teórico necessário para a compreensão do trabalho desenvolvido neste

documento. Já o Capítulo 3 apresenta a metodologia utilizada e suas respectivas as etapas que foram seguidas para a realização deste trabalho. Os resultados do presente estudo são explicados no Capítulo 4. Por fim, o Capítulo 5 apresenta as considerações finais e uma discussão sobre possíveis trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, foram introduzidos os conhecimentos básicos necessários para o estudo. Aqui foram abordados os conteúdos legislativos e técnicos. Este capítulo conta com uma introdução à LGPD e também traz a descrição das vulnerabilidades que serão analisadas.

2.1 Lei Geral de Proteção de Dados Pessoais (LGPD)

Inspirada na *General Data Protection Regulation* (GDPR), regulamentação aplicada na União Europeia (EU) que foi desenvolvida após escândalos envolvendo dados digitais pessoais (RAPÔSO *et al.*, 2019), a LGPD foi desenvolvida com objetivo de proteger os dados pessoais de indivíduos reais. Em uma empresa, por exemplo, isso quer dizer que o foco da LGPD é proteger os dados das pessoas físicas, sejam elas funcionários, clientes e qualquer outro indivíduo que seja impactado pela empresa e, não os dados da empresa em questão.

Sancionada em 14 de agosto de 2018 através do PLC 53/2018 no Congresso Nacional, alterando a Lei 12.965/16 (Marco Civil da Internet), a LGPD entrou em vigor, com 65 artigos, no dia 18 de setembro de 2020 (SÁ *et al.*, 2019).

A LGPD vem sendo bastante discutida, tanto no setor público quanto no privado, além de criar um novo regramento para o uso de dados pessoais tanto no âmbito *online* quanto no *offline* (SÁ *et al.*, 2019).

Em se tratando de dados, a LGPD trata diversas categorias, sendo elas: Dados Pessoais, Dados Sensíveis, Dados Públicos e Dados Anonimizados (BRASIL, 2021). Cada categoria será explicada nas próximas subseções.

2.1.1 Dados Pessoais

São todos os dados que possibilitam a identificação de pessoas naturais de forma direta ou indireta. Nome e sobrenome, data e local de nascimento, Registro Geral (RG), Cadastro de Pessoas Físicas (CPF) são exemplos de dados pessoais.

2.1.2 Dados Sensíveis

São dados pessoais que revelam questões mais ímpares, como raça ou etnia, convicções religiosas ou filosóficas, opiniões políticas e diversas outras informações. Há ainda algumas

observações relacionadas aos dados sensíveis quando se trata de menores de idade, como por exemplo o consentimento indispensável e claro de pelo menos um dos pais ou responsáveis.

2.1.3 Dados Públicos

São, novamente, dados pessoais que tornaram-se públicos pelo titular em um momento anterior e de forma evidente. Para que as organizações usem esses dados é preciso considerar a finalidade, boa-fé e interesse público que justificam a disponibilidade. Caso a organização deseje compartilhar tais dados com outras organizações, é necessário solicitar novamente o consentimento do titular.

2.1.4 Dados Anonimizados

Se trata de uma técnica de tratamento de dados que remove e/ou modifica informações que possam identificar o indivíduo, possibilitando seu anonimato. Caso o dado tratado não garanta o anonimato do titular, ele é considerado um dado pseudonimizado, sujeito à LGPD.

Um exemplo seriam textos de jornais escritos para que não seja possível identificar o indivíduo. Além das técnicas textuais, outras técnicas também podem ser citadas como, por exemplo, a utilização de efeitos sonoros e visuais que impossibilitam a identificação dos indivíduos.

2.2 Aplicações Móveis

Na sociedade atual, é muito comum nos depararmos com indivíduos interagindo com seus *smartphones*. No Brasil, em 2019, cerca de 98,6% dos dispositivos utilizados para acessar a internet são *smartphones* (IBGE, 2019). Para que esses indivíduos possam fazer uso dos dispositivos para os mais diversos fins, é preciso que alguém ou alguma empresa, tenha investido em uma solução, gerando uma aplicação para dispositivos móveis.

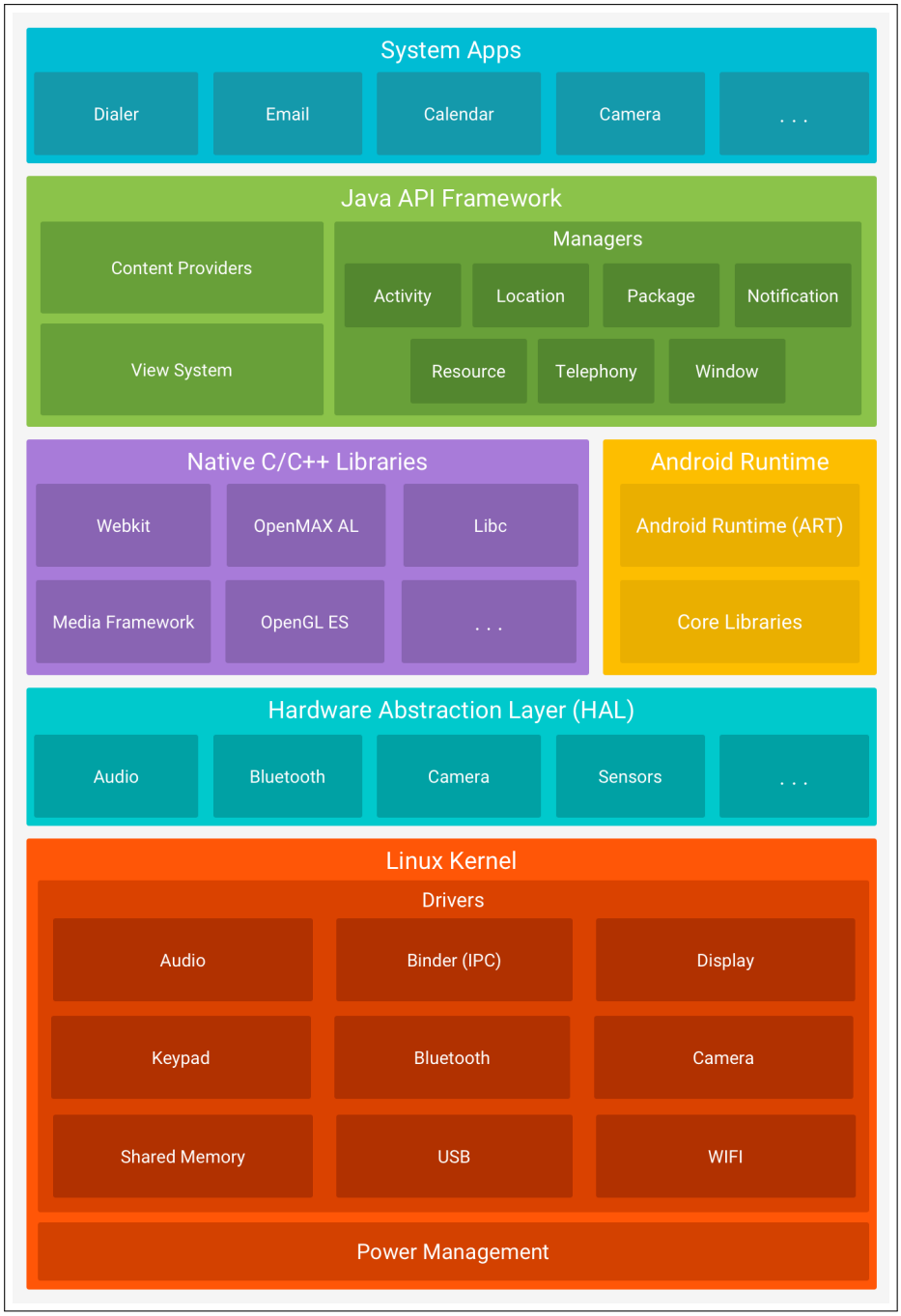
Os aplicativos fazem parte do cotidiano, principalmente em grandes cidades. Em 2019, cerca de 84.4% dos domicílios em regiões urbanas contavam com pessoas que tinham telefone móvel celular para uso pessoal enquanto esse número caia para apenas 59,3% em regiões rurais (IBGE, 2019).

Existem aplicações voltadas a diversas atividades, por exemplo: entretenimento, produtividade, comunicação e outras atividades. Os aplicativos podem ser utilizados para

simplificar o dia a dia (GCF Global, 2018). Inclusive, não é muito difícil que você esteja lendo esse trabalho por um dispositivo móvel.

Dentro dos dispositivos móveis, temos algumas categorias que se destacam, dentre elas estão: *smartphones*, *tablets*, *notebooks*, até mesmo alguns relógios (STUDY.COM, 2020). Neste trabalho iremos focar nos *smartphones*, mais especificamente nos *smartphones* com sistema operacional Android.

Figura 1 – Arquitetura da plataforma Android



Fonte: Android para desenvolvedores (Android Developers, 2023)

A pilha de componentes do Android (Figura 1) conta com um grande número de bibliotecas e aplicações. A grande maioria é construída sobre componentes *open source* como o Kernel Linux, por exemplo. Dessa forma, a contribuição para a plataforma pode vir de desenvolvedores individuais e organizações de terceiros, não se limitando aos engenheiros da Google. Porém, se faz necessária a aprovação de código por meio do sistema de recisão da Google ((DRAKE *et al.*, 2014).

O Android é uma plataforma *open source* para dispositivos móveis desenvolvida pela Google, que possui um *framework* próprio que permite que desenvolvedores possam criar aplicativos sem a necessidade de chegar ao nível mais baixo de abstração. Isto só é possível devido a integração com a *Application Programming Interface* (API) que acessa todas as facilidades que um dispositivo oferece. Assim, o *framework* possibilita a comunicação entre máquina e humano. Este *framework* é executado dentro de uma máquina virtual, o mesmo ambiente onde são executados os aplicativos desenvolvidos (DRAKE *et al.*, 2014)

2.3 Vulnerabilidades

Com a quantidade de dispositivos móveis cada vez mais crescente, é comum surgir a preocupação com os dados pessoais. Por isso é importante discutir sobre as vulnerabilidades que os dispositivos Android podem apresentar.

Antes de analisar as vulnerabilidades, é importante ressaltar que existem dois ambientes onde a vulnerabilidade pode existir: cliente e servidor. O lado do cliente (*Client-Side*) é responsável por fazer a interação com o usuário. É nela onde se encontram as telas dos aplicativos.

Já o lado do servidor (*Server-Side*) é responsável por tratar os dados inseridos pelo usuário e interagir com os demais serviços, como banco de dados, por exemplo. Neste lado do serviço, o desenvolvedor tem mais autonomia para gerir a segurança do aplicativo. Há diversas boas práticas que podem ser seguidas para garantir uma conexão segura.

Dito isto, cerca de 60% das vulnerabilidades em dispositivos móveis com o sistema operacional Android ocorrem no *Client-Side*, 89% são exploradas sem acesso físico e 56% sem acesso de administrador (CASEY, 2019). A partir desses dados, podemos inferir que o usuário tem um papel importante na segurança dos dados. Na sequência serão apresentadas as sete maiores vulnerabilidades em aplicativos Android em 2022, segundo Casey (CASEY, 2019).

2.3.1 Proteção Binária

Jailbreak é o processo de exploração de falhas de um dispositivo eletrônico bloqueado para instalação de aplicativos de terceiros, que não foram disponibilizados pela fabricante do dispositivo. Através dessa técnina, o usuário do dispositivo adiquiri acesso total à raiz do sistema e todos os recursos. A denominação se dá pois liberta os usuários da "prisão"que são as limitações existentes (KASPERSKY, 2023).

Quando um dispositivo passa pelo processo conhecido como *root* ou *jailbreak*, a proteção de dados e a criptografia do sistema são contornados. Quando isso ocorre, qualquer código malicioso pode ser executado no dispositivo, o que pode alterar os comportamentos esperados pela lógica implementada no aplicativo. Ferramentas forense utilizadas para recuperação de dados geralmente são executadas em dispositivos com *root*.

A recomendação é não executar aplicativos em dispositivos com *root* ou *jailbreak*. Também é possível criar alguma verificação no aplicativo para identificação de *root* ou *jailbreak*. Essa etapa de verificação pode ajudar a mitigar os riscos e proteger os dados dentro do aplicativo, para evitar que sejam expostos.

2.3.2 Proteção insuficiente da camada de transporte

É comum que haja falhas em aplicativos ao criptografar os dados da rede quando é necessário uma proteção de dados confidenciais. É importante que os dados das transações em páginas *web* sejam criptografados, incluindo conexões de *back-end*, para não expor dados de autenticação ou *tokens* de sessão, por exemplo. As conexões de *back-end* ainda podem apresentar um risco menor de ataque, mas devem ser consideradas pois podem resultar em comprometimento de contas de usuários e levar ao vazamento das suas informações.

Para que se possa mitigar os riscos dessa vulnerabilidade, é importante que dados confidenciais, como números de cartão de crédito e informações de saúde, sejam criptografados. Aplicativos que trafegam esses dados como textos simples são considerados vulneráveis pois apresentam falhas que podem ser atacadas por invasores.

2.3.3 Autorização/Autenticação insuficiente

Autorização insuficiente ocorre quando o aplicativo não é capaz de executar verificações adequadas de autorização, isso gera uma inconsistência ao acessar os dados, ferindo a

política de segurança. A autorização é responsável por orquestrar o que um usuário, serviço ou aplicativo pode fazer no sistema.

Um esquema de estrutura de autorização comprovada, consiste em manter uma lógica de autorização e autenticação consistente e segura. Para isso, é preciso que a estrutura tenha sido testada e validada pelos desenvolvedores. É recomendado que uma estrutura de autorização seja implementada no aplicativo, que destaque os arquivos de configuração e, que sejam baseados em políticas de autorização.

2.3.4 Validação de certificado imprópria de criptografia

Quando o aplicativo não está validando certificados *Secure Sockets Layer* (SSL) e/ou *Transport Layer Security* (TLS) corretamente ou usa um sistema de validação que não verifica novamente se o provedor confiável emitiu o certificado, ocorre a vulnerabilidade de validação imprópria de criptografia. O correto é o aplicativo estar configurado para encerrar a conexão quando houver essa vulnerabilidade. Qualquer dado trocado em um aplicativo que não consegue fazer essas validações pode ser exposto a acesso não autorizado.

Para mitigar problemas com a verificação dos certificados é necessário que o aplicativo esteja validando corretamente os certificados com uma fonte confiável, como uma Autoridade de Certificação.

2.3.5 Força Bruta - Enumeração do Usuário

Um ataque de força bruta é um método utilizado para determinar um valor desconhecido, utilizando de um processo automatizado para tentar um grande número de possíveis valores. O ataque leva vantagem em cima do fato da entropia do valor ser menor que a percebida.

Por exemplo, enquanto uma senha de 8 caracteres alfanuméricos tem 2,~~8 trilhões de possíveis valores, muitas pessoas irão escolher suas senhas a partir de um pequeno grupo de caracteres contendo palavras e termos comuns. Se há diferentes mensagens de erro de acordo com a combinação de nome de usuário e senha, o responsável pelo ataque pode determinar nomes de usuários ou endereços de *email* baseados nas mensagens de erro.

Geralmente esse tipo de vulnerabilidade ocorre nas funcionalidades de *login*, registro e recuperação de senha. A aplicação não deverá revelar quando o nome de usuário ou *email* for válido. Ao invés da mensagem conter "Desculpe, senha inválida", é recomendado um erro mais genérico como: "Desculpe, seu usuário ou senha estão incorretos. Tente novamente."

2.3.6 Expiração de Sessão Insuficiente

Depois de um usuário realizar o procedimento de encerramento de sessão em um aplicativo, é comum supor que a sessão foi, de fato, finalizada. Porém, se ocorrer alguma falha ao finalizar a sessão, a aplicação fica vulnerável a um ataque onde um usuário mal intencionado pode assumir a identidade de outro e realizar ações em seu nome.

A melhor forma de mitigar essa vulnerabilidade, é garantir que, na aplicação, exista um botão ou algo similar para finalizar a sessão do usuário. Assim como, garantir que a funcionalidade esteja consistente e funcional.

2.3.7 Vazamento de informações - Cache de aplicativo

Dados sensíveis armazenados em *cache* podem ser vazados, tanto através da aplicação principal quanto por meio de códigos de terceiros. Garantir a segurança dos dados é um desafio para os dispositivos móveis. Roubo e perda de dispositivos, falta de bloqueio por senha ou similares são alguns dos cenários onde os dados podem ser facilmente vazados.

É importante validar que os dados confidenciais não vazem acidentalmente por *cache*. Os desenvolvedores podem prevenir criando modelos de ameaça para sistemas operacionais, bibliotecas de terceiros e verificar a forma como os dados são armazenados nos *caches* de URL, pressionamento do teclado, *logs*, área de transferência e vários outros que são enviados para servidores ou outros aplicativos.

2.4 Segurança em aplicações móveis

Como estamos estudando vulnerabilidades é importante, também, estudarmos segurança em aplicações móveis de um modo geral. Aqui iremos trazer alguns conceitos de segurança, além de discutir a importância de uma senha segura.

2.4.1 Segurança da informação

Quando se fala em segurança em aplicações móveis, falamos também da segurança do código fonte desenvolvido. Tal código pode seguir diversos princípios de segurança, mas existem três que são indispensáveis, são eles: confidencialidade, integridade e disponibilidade (HINTZBERGEN *et al.*, 2018). A Figura 2 ilustra como os conceitos apresentados se relacionam

entre si, também fica visível que a segurança da informação se dá na interseção deles. A Tabela 1 define os conceitos de segurança.

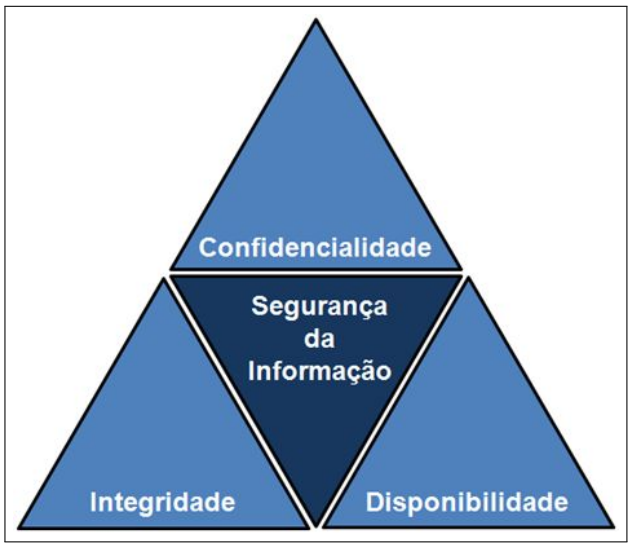
2.4.2 Autenticação por senha

A senha é um método comum de autenticação. Consiste em um identificador composto por uma sequência de caracteres. Essa sequência, levando em conta letras minúsculas, maiúsculas e dígitos, possui 56.800.235.584 possibilidades para uma sequência de 6 caracteres e, ao contarmos com os 95 caracteres imprimíveis da tabela *American Standard Code for Information Interchange* (ASCII), esse número aumenta para 735.091.890.625 (ROCCIA, 2021).

A forma como a senha será armazenada é uma etapa muito importante na autenticação. Uma abordagem básica seria salvar a senha como texto simples, porém se houver vazamento de informações, a conta e privacidade dos usuários afetados serão comprometidas.

Uma alternativa seria criptografar as senhas antes de armazená-las. Dessa forma as senhas estarão protegidas de possíveis ataques. Vale mencionar que se o segredo para descriptografar as senhas também for vazado, os usuários ainda estarão sujeitos aos malefícios do vazamento. Tais malefícios podem incluir vazamento de dados pessoais, dados privados, dados sensíveis e a perda do acesso ao aplicativo e demais informações do usuário.

Figura 2 – Segurança da Informação, princípios básicos, Confidencialidade, Integridade e Disponibilidade.



Fonte: PSI – Política de Segurança da Informação (LOPES, 2017)

Princípio	Responsabilidade
Confidencialidade	Garantir que as informações sejam entregues apenas ao seu destinatário. Nenhum outro usuário do sistema, ou qualquer pessoa que tenha acesso ao meio em que elas são transmitidas deve poder visualizá-las. A solução mais comum para garantir a confidencialidade é o uso autenticação aliado à criptografia.
Integridade	A informação a ser transmitida deve chegar ao seu destino de maneira intacta, sem alterações ou ruídos. A integridade de um sistema pode ser comprometida por *malwares* inseridos por um atacante. Para evitar que isso aconteça pode ser feita a detecção de intrusão ou o uso de *hashing*.
Disponibilidade	A disponibilidade é garantida quando os três aspectos a seguir são obedecidos: • Oportunidade: Informação disponível quando solicitado; • Continuidade: Permitir o acesso, mesmo que parcial, em caso de falhas; • Robustez: Ter a capacidade de oferecer acessos simultâneos conforme a demanda.

Tabela 1 – Fundamentos da Segurança da Informação

3 METODOLOGIA

A primeira etapa da pesquisa será dividida em três partes: i) elaborar um tema de pesquisa que determina uma área de conhecimento na qual se deseja trabalhar; ii) realizar uma revisão bibliográfica; e iii) definir o objetivo da pesquisa. Esta primeira etapa da metodologia será de grande importância na identificação da relevância do tema. Além disso, também ajudará no delineamento do escopo da pesquisa por meio dos objetivos, geral e específicos.

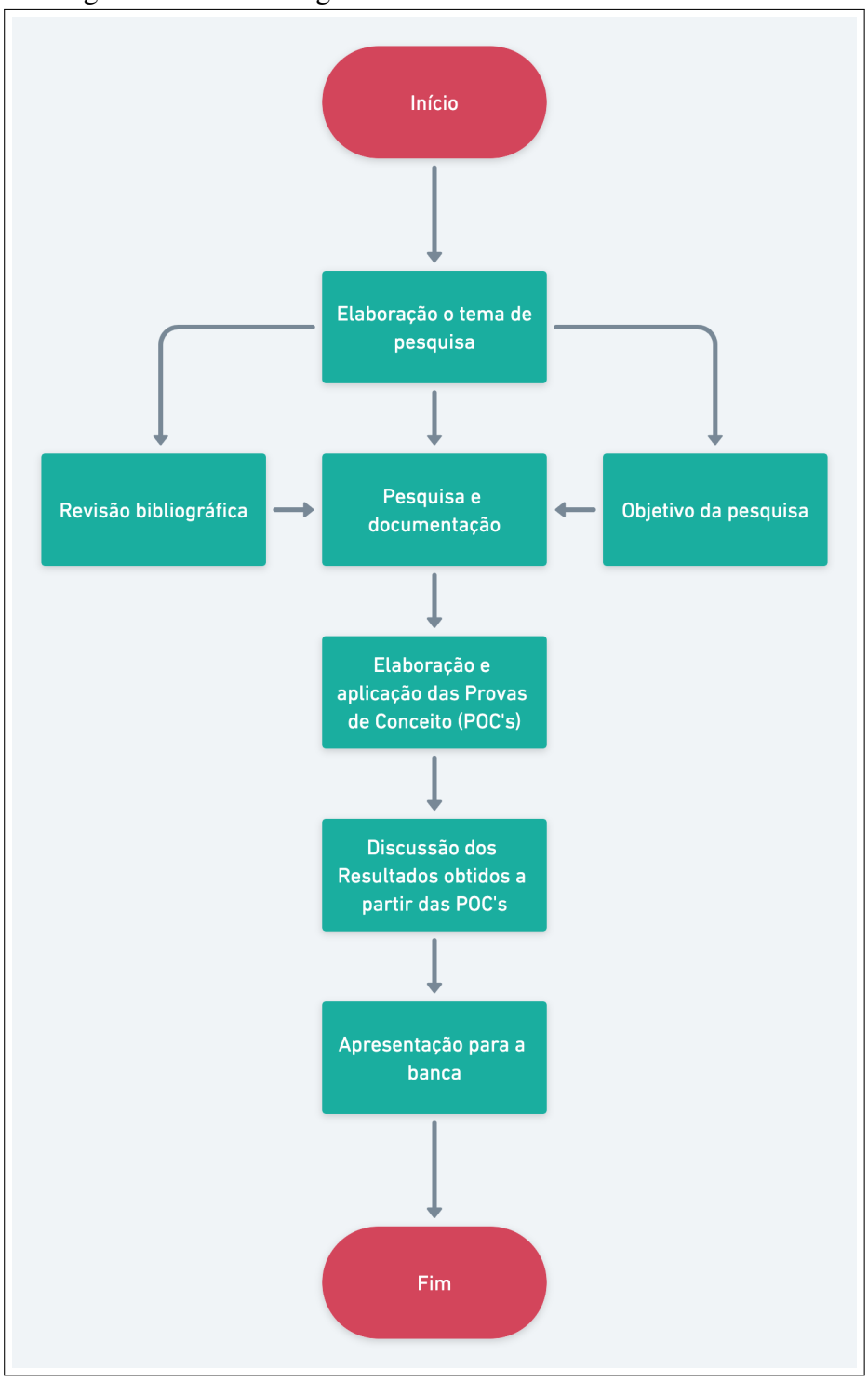
Em relação aos aspectos de caracterização e natureza, a pesquisa será de cunho exploratório e experimental. Pesquisas exploratórias têm como objetivo principal o aprofundamento de ideias ou a descoberta de intuições (GIL, 2002). Segundo Gil (2002) grande parte das pesquisas exploratórias envolvem: i) levantamento bibliográfico; ii) entrevistas com indivíduos que tiveram experiências práticas com o problema pesquisado; e iii) análise de exemplos que estimulem a compreensão. Neste trabalho, a natureza da pesquisa exploratória será utilizada para introduzir os conceitos básicos necessários para a compreensão do problema e o objetivo da pesquisa, além de descrever, mais detalhadamente na Fundamentação Teórica, o que é a LGPD, o que são aplicações móveis para dispositivos Android, as vulnerabilidades mais comuns no sistema Android e os motivos das suas escolhas. A maior parte da utilização da pesquisa exploratória, neste trabalho, será por meio do levantamento bibliográfico. Portanto, a segunda etapa da metodologia utilizará a pesquisa exploratória para reunir toda a estrutura teórica e os conhecimentos necessários para o entendimento do tema em questão.

No que diz respeito ao método, esta pesquisa também se caracteriza como uma pesquisa experimental. Uma pesquisa experimental implica que o investigador, de forma sistemática, fará alterações no ambiente ou objeto a ser pesquisado de forma a observar se cada intervenção produz os resultados esperados (WAZLAWICK, 2009). Sendo assim, algumas provas de conceito de aplicativos Android serão elaboradas no intuito de mostrar a vulnerabilidade dos dados pessoais. Para aplicar as provas de conceito, será utilizado o aplicativo Imuni, que será apresentado e detalhado nos próximos capítulos. Dentro de cada tela analisada, seram discutidas formas como a vulnerabilidade poderia ocorrer e como a LGPD poderia ajudar a mitigar tais vulnerabilidades.. A partir dessas provas de conceito, será possível elaborar um documento guia que possa mitigar ou eliminar vulnerabilidades destacadas em cada prova de conceito elaborada. Portanto, a terceira e última etapa utilizará da pesquisa experimental para reunir informações necessárias para discussão a respeito de leis relacionadas aos dados pessoais e como elas se comunicam com o desenvolvimento mobile em *smartphones* Android.

Todo o processo descrito pode ser visualizado na Figura 3. O fluxograma conta com as etapas descritas acima, além de possibilitar uma estimativa de conclusão e o passo a passo seguido para o presente estudo.

Vale ressaltar que é possível notar um paralelismo nas atividades, isso possibilitou que o estudo sofresse uma aceleração positiva, encurtando o tempo total de desenvolvimento do trabalho.

Figura 3 – Fluxograma da Metodologia



Fonte: Elaborado pelo autor (2022)

4 RESULTADOS

Neste capítulo será apresentado o aplicativo utilizado para a análise das vulnerabilidades. Aqui serão discutidas as formas como as vulnerabilidades poderiam ocorrer em cada tela apresentada. A primeira parte deste capítulo traz, de forma detalhada, as telas do aplicativo. Na segunda parte, encontra-se a discussão destas telas sob a ótica das vulnerabilidades estudadas e, por fim, como a LGPD poderia mitigar estas vulnerabilidades

Os resultados encontrados após a aplicação das Provas de Conceito, descritas a seguir, foram discutidos e analisados em relação aos aspectos da LGPD.

4.1 Prova de Conceito (PoC)

Imuni, um aplicativo desenvolvido em 2020 na cadeira de Projeto Integrado II do curso de Sistemas e Mídias Digitais com a equipe Ignilab, é uma carteira de vacinação digital, onde o usuário pode cadastrar e acompanhar o histórico de vacinas, assim como status de imunidade.

Em 2020, o Brasil enfrentava a pandemia da COVID-19 e, diante desse contexto pandêmico, o aplicativo Imuni foi desenvolvido. A aplicação conta com um sistema de cadastro de usuários, bem como o login e o cadastro de vacinas. É possível realizar o cadastro de todas as vacinas aplicadas anteriormente, guardando um histórico de vacinas e, também adicionar novas aplicações. Existe a opção de compartilhar o registro das vacinas, afim de encorajar outras pessoas a se vacinarem.

O aplicativo em questão foi escolhido por se tratar de um aplicativo Android. Além disso, ferramentas relacionadas à área da saúde necessitam de uma atenção maior, por se tratar de dados sensíveis.

4.1.1 Tela de login

O aplicativo conta com a tela de *login*, Figura 4, onde o usuário será convidado a inserir os dados para acessar sua conta, os dados são: *e-mail* e senha.

A tela é composta pela logo do aplicativo, seguido dos campos de inserção dos dados. Logo abaixo podemos verificar o botão responsável por efetivar o *login*. Existe um espaço dedicado à criação de novas contas, contando com um texto questionando a existência do cadastro e um botão que leva para a tela de cadastro. Por fim, a tela possui um *link* para os casos

de senhas esquecidas. Toda a descrição está ilustrada na Figura 4.

Figura 4 – Tela de *login*

Fonte: Elaborado pelo autor (2022)

Nesta tela existe a verificação de credenciais, onde a aplicação informa um erro, caso o usuário não esteja cadastrado ou suas credenciais estejam incorretas (Imagem 5). Tais erros devem ser explorados e testados de forma consistente para que não haja vulnerabilidades.

Figura 5 – Tela de erro no *login*

Fonte: Elaborado pelo autor (2022)

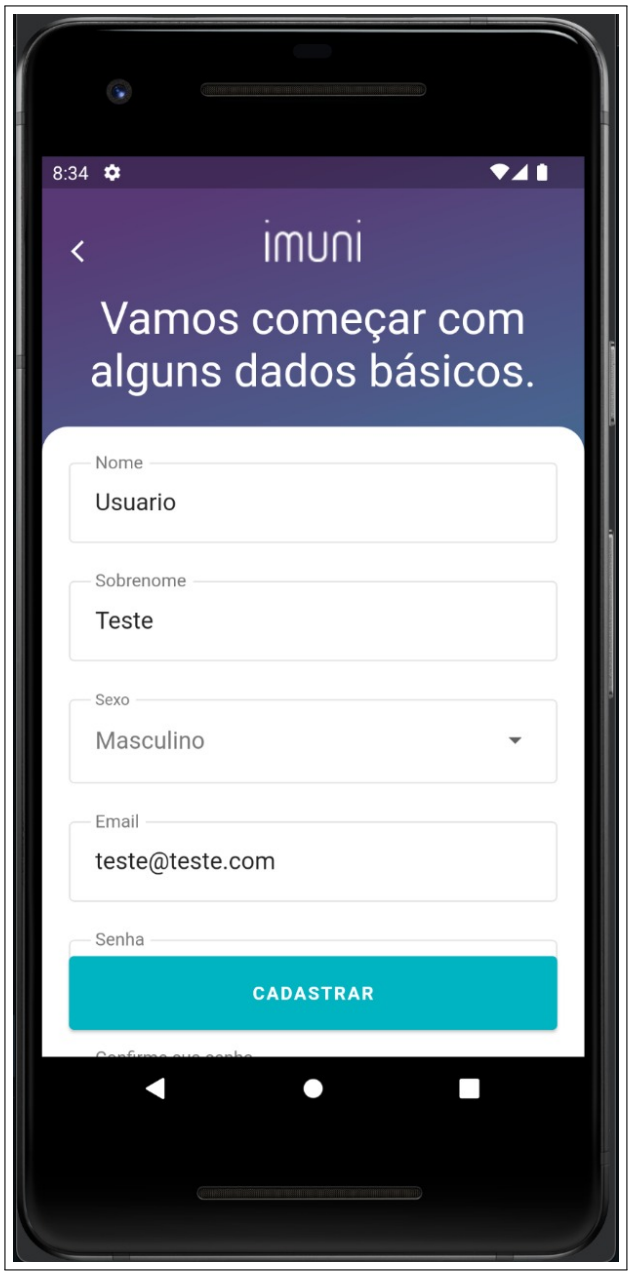
4.1.2 Tela de cadastro

Nesta tela o usuário é convidado para criar um novo cadastro. Para criar é preciso informar alguns dados, são eles: nome, sobrenome, sexo, *e-mail* e senha.

Na tela, existe um texto descritivo informando que alguns dados são necessários, seguido do formulário com os campos indispensáveis para o cadastro. No fim da tela, é possível visualizar o botão responsável por efetivar o cadastro da nova conta, com o título "cadastrar". A descrição é ilustrada na Figura 6.

É importante salientar que o campo de senha é acompanhado do campo de confirma-

Figura 6 – Tela de cadastro



Fonte: Elaborado pelo autor (2022)

ção de senha, este tem a finalidade validar se as duas senhas, inseridas pelo usuário, coincidem. Garantir que a senhas digitadas sejam idênticas ajuda na prevenção de vulnerabilidades. Caso as senhas não atendam aos requisitos de validação, um erro é mostrado ao usuário, conforme a Figura 7 ilustra.

4.1.3 Tela de boas vindas

Esta tela, tem como finalidade dar as boas vindas ao usuário. Conta com acesso rápido ao cadastro de novas vacinas, bem como o compartilhamento da carteira de vacinação

Figura 7 – Tela de erro no cadastro

Fonte: Elaborado pelo autor (2022)

digital e um menu de opções.

A tela conta com uma ilustração inicial, informando ao usuário que não existem vacinas cadastras ainda e convida para realizar o cadastro da primeira vacina. Do lado esquerdo é possível notar um típico ícone de menu sanduíche, utilizado amplamente nos mais diversos aplicativos. À direita encontra-se o botão destinado ao compartilhamento da carteira de vacinação. A ilustração descrita pode ser vista na Figura 8.

As telas adicionais comentadas acima serão discutidas nos subtópicos a seguir.

Figura 8 – Tela inicial

Fonte: Elaborado pelo autor (2022)

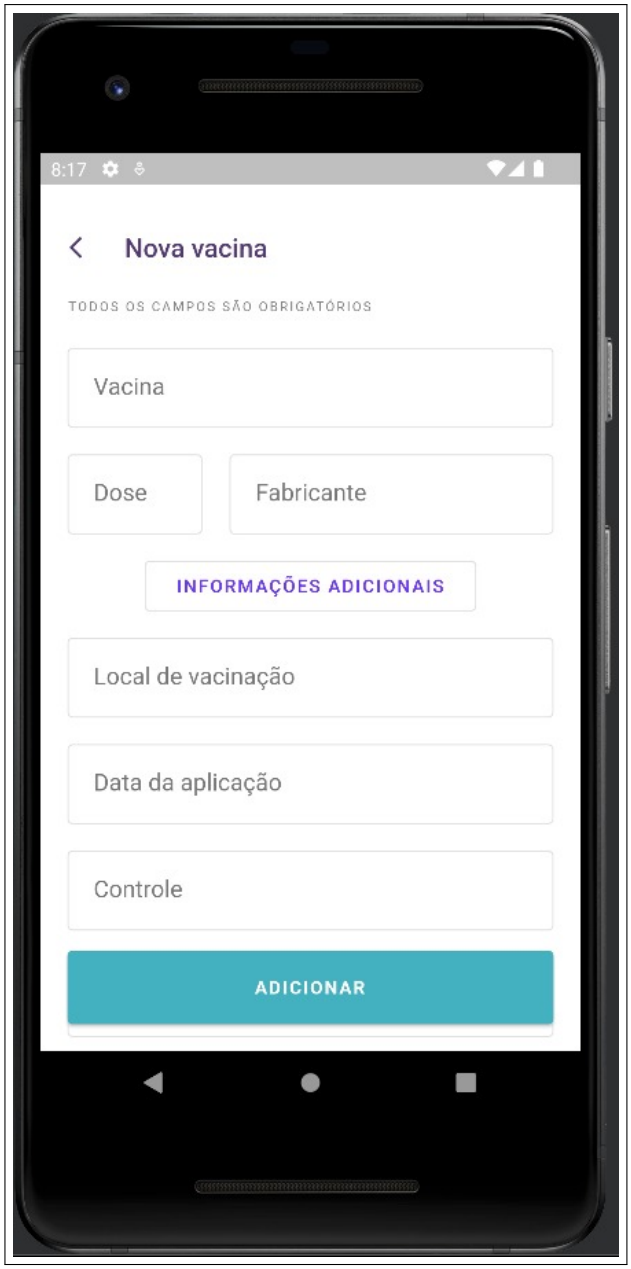
4.1.4 Tela de cadastro de vacina

Esta tela (Imagem 9) é responsável pelo cadastro de novas vacinas. Para adicionar um novo registro de vacinação, o usuário deve preencher as informações básicas da vacina, são elas: nome da vacina, dose, fabricante, local de vacinação, data da aplicação, controle e lote.

A tela é constituída por um formulário, que contém os dados da vacina, um botão responsável por efetuar o cadastro e enviar a informação para o *back-end* e um botão de navegação, que se encontra na parte superior esquerda, responsável por levar o usuário para a tela de boas vindas (Figura 8) ou, se houver vacinas cadastras, a tela de listagem de vacinas

(Figura 10).

Figura 9 – Tela de cadastro de vacina



Fonte: Elaborado pelo autor (2022)

4.1.5 Tela de listagem de vacinas

Nesta tela (Imagem 10) é possível visualizar todas os registros de vacinas cadastrados pelo usuário, além de sinalizar o status de imunização daquele usuário.

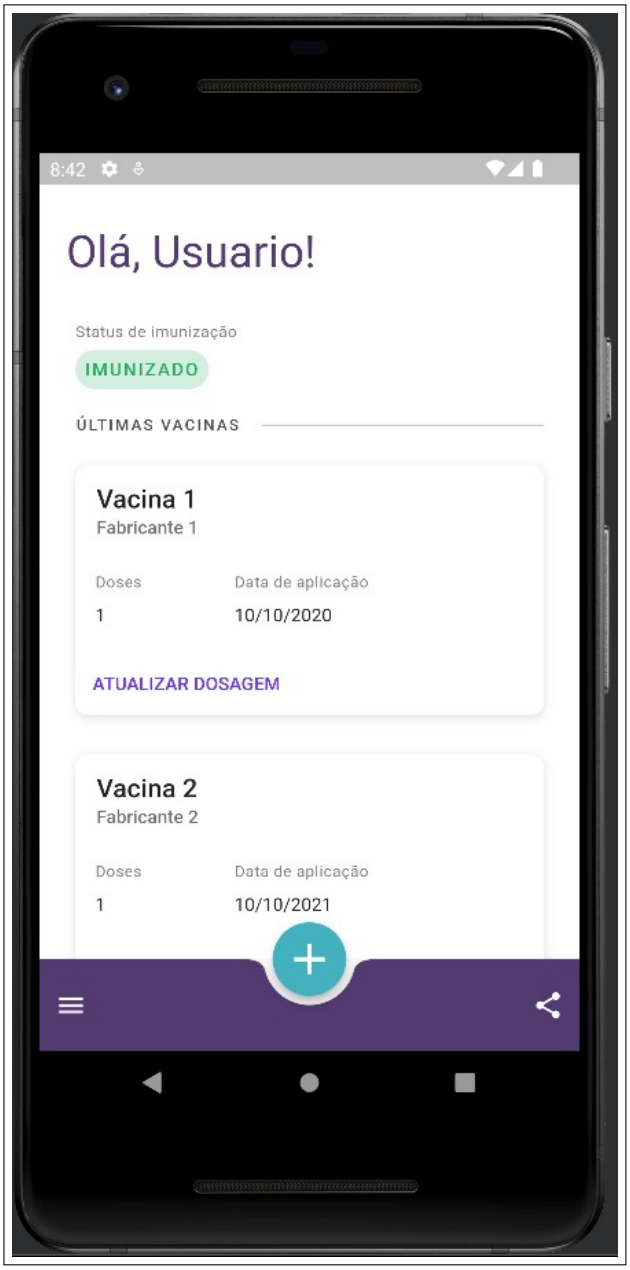
A tela é conta com o status de imunização, como já foi citado, e a listagem, em ordem de cadastro, das vacinas registradas. Cada registro conta com as informações básicas da

vacina, como o nome, fabricante, dose e a data da aplicação.

Também existe um menu de navegação que se encontra na parte inferior do aplicativo, nele existem as opções de acessar o menu lateral, compartilhar o registro de vacinas e situação vacinal e cadastrar um novo registro de vacina.

O usuário também pode atualizar os dados das vacinas, através do botão intitulado com "ATUALIZAR DOSAGEM". O usuário será levado para uma tela semelhante à tela de cadastro de vacina (Imagem 9) mas com os dados da vacina selecionada para realizar a atualização.

Figura 10 – Tela de listagem de vacinas



Fonte: Elaborado pelo autor (2022)

4.1.6 Outras telas

Existem outras telas na aplicação, como a de menu e visualização do conteúdo que será compartilhado. Tais telas não sofrerão impactos com os testes propostos pelo presente estudo, por isso sua descrição detalhada não se faz necessária nesse momento.

Na Figura 11 podemos ver a tela de menu e a Figura 12 é a tela de visualização do conteúdo que será compartilhado. O compartilhamento da carteira de vacinação se faz importante pois incentiva os familiares e amigos próximos a se vacinarem.

4.2 Análise sobre o impacto da LGPD na PoC

Esta seção é dedicada para entender como as vulnerabilidades poderiam acontecer nas telas apresentadas e como seria possível mitigar a incidência dessas vulnerabilidades. Para isso, esta seção será dividida em subseções para cada vulnerabilidade explorada, quando aplicável.

É sabido que ferramentas relacionada à área da saúde trafegam e armazenam dados sensíveis dos usuários, por isso, qualquer vulnerabilidade aqui apresentada poderia gerar riscos incalculáveis aos seus usuários.

Abaixo veremos como cada uma das vulnerabilidades analisadas poderia gerar danos ao usuário e como a equipe de desenvolvedores e o próprio usuário podem mitigar estes acontecimentos. É importante notar que algumas das atitudes aqui mencionadas são de fácil aplicação tanto para a equipe de desenvolvimento quanto para o usuário final.

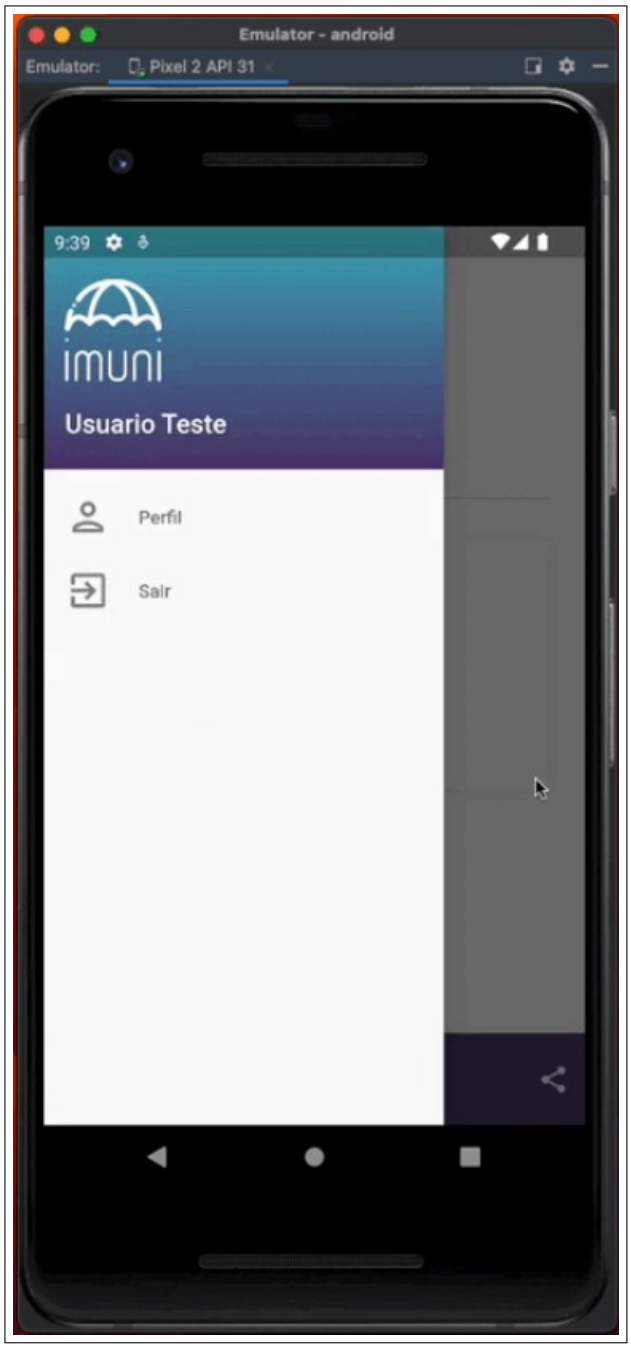
4.2.1 Proteção insuficiente da camada de transporte

Para que o usuário possa cadastrar novos registros e realizar o login no aplicativo, é preciso uma troca de informações com o servidor *back-end*. Caso essas informações não sejam criptografadas antes de serem enviadas para o servidor, existe a possibilidade de serem interceptadas e, consequentemente, exploradas ou vazadas.

Aplicativos que contenham informações de saúde merecem uma atenção a mais, por se tratar de dados sensíveis. Por isso, se faz necessária a criptografia dos dados. Em hipótese alguma os dados devem ser enviados como texto simples para o *back-end*.

As telas de *login* (Figura 4) e cadastro de usuário (Figura 6) contém informações importantes que permitem o acesso ao aplicativo. Logo, essas informações devem ser criptografadas.

Figura 11 – Tela de menu

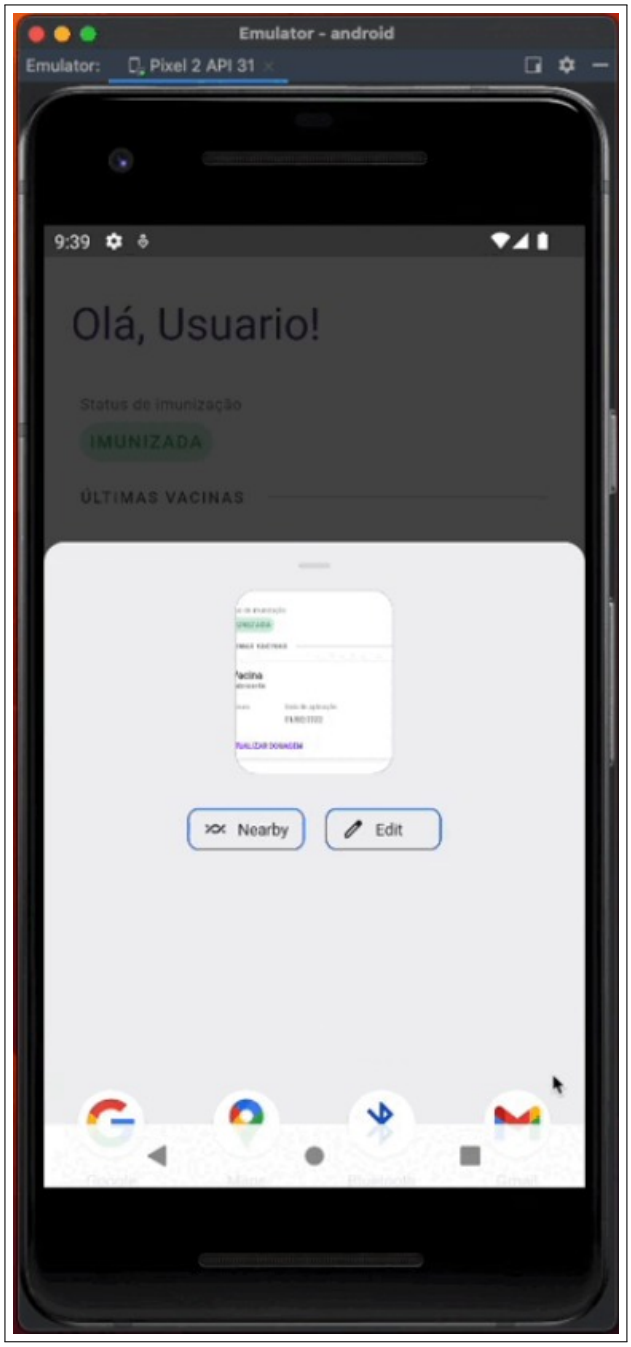


Fonte: Elaborado pelo autor (2022)

Na tela de cadastro de vacinas (Figura 9) existem informações sensíveis sobre a saúde do usuário e, por isso, também devem ser criptografadas ao se comunicar com o *back-end*.

O desenvolvedor precisa utilizar mecanismos eficazes de criptografia, garantindo uma maior segurança aos dados dos usuários da aplicação.

Figura 12 – Tela de compartilhamento da carteira de vacinação



Fonte: Elaborado pelo autor (2022)

4.2.2 Autorização/Autenticação insuficiente

A tela de *login*, Figura 4, é responsável pela autenticação do aplicativo, esta tela deve ser fortemente protegida pois, se sofrer um ataque, pode garantir acesso indevido.

Caso o ataque seja bem sucedido os dados do usuário e informações sobre sua saúde (vacinas tomadas, estado da imunidade, etc.), no caso da aplicação analisada, estarão sujeitos à vazamentos ou até mesmo utilizados para os mais diversos fins maliciosos. Vale ressaltar que a

tela de *login* (Figura 4) é a porta de entrada do aplicativo, por isso, a segurança deve ser dobrada nesta etapa.

Além da criptografia citada anteriormente, esta tela pode conter mais métodos de segurança. Uma forma de garantir a segurança é utilizando autenticação de dois fatores, onde o aplicativo utiliza de outros serviços, como *e-mail* ou mensagem de texto, para validar a autenticidade do usuário.

4.2.3 Força Bruta - Enumeração do Usuário

Um outro tipo de ataque que afeta a tela de *login*, Figura 4, é o de força bruta. Este ataque consiste em determinar um valor desconhecido, como a senha por exemplo, a partir de um grande número de tentativas com valores diversos.

Senhas de baixa complexidade tem mais chances de serem quebradas por esse método. Por isso, é importante que o usuário sempre garanta uma alta complexidade na senha, além de utilizar os mais diversos caracteres possíveis.

Outra forma de mitigar esse ataque é definindo um número máximo de tentativas para que a conta seja bloqueada, podendo ser recuperada posteriormente por métodos mais seguros.

Um *feedback* especificando qual campo é incorreto, em alguns casos pode não ser interessante. Na tela de *login* (Imagem 4), por exemplo, o uso de mensagens de erro específicas é desencorajado, uma vez que informar qual das informações está incorreta pode gerar um efeito contrário ao desejado, ajudando a explorar a vulnerabilidade. Informar, por exemplo, que a senha está incorreta confirma que o *email* inserido está cadastrado na plataforma, o que não é interessante quando se fala de segurança e exploração de vulnerabilidades.

É importante que o desenvolvedor use de mensagens genéricas de erro, para que não seja possível identifica se a informação inserida existe ou não no banco de dados. Na Figura 5 é possível ver o uso correto das mensagens de erro genéricas.

Outro método que pode ajudar a minimizar a ocorrência dessa vulnerabilidade, é o de exigir uma complexidade mínima da senha. Por exemplo, é muito comum que, ao preencher uma senha, o usuário seja obrigado a inserir diversas combinações de caracteres, letras minúsculas e maiúsculas, números e símbolos garantem uma senha forte e mais difícil de ser quebrada.

Aidcionar validade nas senhas também garantem uma maior segurança ao usuário. Definir o tempo de vida de uma senha garante que o usuário sempre mude sua senha, garantindo,

ainda mais, uma menor chance de ser quebrada.

4.2.4 Expiração de Sessão Insuficiente

Existe uma vulnerabilidade que consiste em explorar a sessão ativa do usuário. Ela acontece principalmente pela falta de um funcionalidade responsável por finalizar a sessão ou alguma inconsistência ao realizar o procedimento de finalização de sessão.

Por isso, o aplicativo deve garantir que a finalização da sessão foi efetuada de forma correta, caso contrário, o usuário estará sujeito a um ataque e o sujeito malicioso pode ganhar um acesso indevido, obtendo informações sensíveis do usuário.

A existência de áreas específicas para que o usuário possa finalizar a sessão é de extrema importância para mitigar essa vulnerabilidade.

Também pode-se definir *tokens* de expiração para que a sessão tenha um prazo de validade. São amplamente utilizados pelos desenvolvedores para garantir segurança e não solicitar a senha a cada vez que o usuário usar o aplicativo, pois isso gera uma complexidade a mais e pode aumentar a frustração do usuário.

4.3 Como a LGPD ajudou a aumentar a privacidade e proteção de dados pessoais

Com as telas detalhadas e as vulnerabilidades discutidas, foi possível analisar e discutir como cada uma das vulnerabilidades poderiam ser mitigadas ao aplicar conceitos e técnicas da LGPD.

Depois de aplicadas as provas de conceito, foi possível identificar que ao aplicar algumas práticas discutidas na LGPD os riscos de ataques podem ser mitigados.

No que diz respeito à complexidade e segurança da senha, pôde-se observar que a aplicação de pequenas técnicas já garantem uma senha mais segura. Tais técnicas consistem em solicitar que o usuário use uma quantidade mínima de caracteres na senha, além de utilizar diferentes caracteres para sua construção.

Conhecer o aplicativo ao qual está interagindo também é de grande importância, pois previne que o uso desta ferramenta não trará problemas para os dados utilizados.

Ao utilizar um aplicativo, é importante também que o usuário se certifique que algumas funcionalidades estejam aplicadas e funcionais. Um exemplo seria a função de encerrar a sessão, que, como já foi discutido, pode gerar uma vulnerabilidade para o usuário.

Na perspectiva dos autores, a responsabilidade de uso da aplicação é compartilhada tanto com a equipe de desenvolvimento quanto com o cliente final. Claro, a equipe de desenvolvimento tem deveres a cumprir e deve garantir um sistema confiável. Mas, da parte do usuário, é preciso que este siga atento e desconfie de ações maliciosas.

É sempre importante que o aplicativo disponibilize documentos referentes aos termos e condições, e que usuário leia com atenção tais termos.

5 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho investigou aspectos da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em aplicações móveis na intenção de mitigar ou eliminar possíveis vulnerabilidades de dados.

Para isso, estudou-se a LGPD, os aspectos de desenvolvimento de aplicações móveis e as vulnerabilidades mais recorrentes em *smartphones* Android. Verificou-se os aspectos da LGPD que podem ser adotados em aplicações móveis. Discutiu-se, também, como a LGPD pode aumentar a privacidade e proteção de dados pessoais em aplicações móveis por meio de provas de conceito.

Após toda a discussão vista nas seções anteriores, é possível notar um padrão para mitigar as vulnerabilidades analisadas. Este padrão consiste em manter uma determinada linha de qualidade da aplicação, uma empresa séria não deveria permitir que falhas simples ocorressem em seus aplicativos.

Também foi discutido que o usuário final tem um papel importante quando se trata de complexidade de senhas no uso dos aplicativos. É muito importante que as senhas utilizadas nos aplicativos sejam de alta complexidade, evitando que agentes maliciosos invadam pela "porta da frente". Além disso, o usuário final deve estar atento aos termos e condições disponibilizados pelo aplicativo.

Com a LGPD sendo o foco para essa análise, foi percebido que muitas das ações que devem ser tomadas são, relativamente, simples de serem aplicadas.

Como trabalhos futuros, pode-se seguir o estudo de caso em aplicações mais específicas, ou seja, de outros domínios. Outro possível trabalho futuro é, a partir das diretrizes da LGPD, elaborar um *benchmark* para fazer uma avaliação automática ou semiautomática das vulnerabilidades.

A análise de outras leis e diretrizes relevantes para a segurança em dispositivos móveis pode ser discutida e aplicada assim como a LGPD foi discutida neste estudo.

Por fim, uma versão para iOS seria interessante para ampliar o uso do estudo proposto neste documento.

Vale ressaltar que há um universo de possibilidades que podem ser continuadas a partir deste trabalho. Manter este estudo atualizado pode ajudar a encontrar pontos de melhoria na própria LGPD. Também é possível que, a partir deste estudo e estudos derivados, melhorias nos sistemas operacionais existentes e testados possam acontecer. Dito isto, os trabalhos derivados

deste estudo podem trazer grandes impactos positivos para empresas e usuários de dispositivos móveis.

REFERÊNCIAS

Android Developers. **Arquitetura da plataforma**. 2023. Disponível em: <https://developer.android.com/guide/platform?hl=pt-br>. Acessado em 4 de janeiro de 2023.

BAGATINI, J. A.; GUIMARãES, J. A. C.; SANT'ANA, R. C. G. Gerenciamento dos dados pessoais em arquivos: uma perspectiva centrada no indivíduo com base na lgpd. **Acervo**, v. 34, n. 3, p. 1–20, nov. 2021. Disponível em: <https://revista.an.gov.br/index.php/revistaacervo/article/view/1749>.

BRASIL. **Ministério da Cidadania. Classificação dos Dados**. 2021. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acessado em 27 de abril de 2022.

CASEY, K. **Top 7 Vulnerabilities In Android Applications 2022**. 2019. Disponível em: <https://codersera.com/blog/top-7-vulnerabilities-in-android-applications-2019/>. Acessado em 26 de setembro de 2022.

Cetic.br. **Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br**. 2021. Disponível em: <https://www.cetic.br/pt/pesquisa/tic-covid-19/indicadores/>. Acessado em 4 de janeiro de 2023.

DRAKE, J. J.; LANIER, Z.; MULLINER, C.; FORA, P. O.; RIDLEY, S. A.; WICHERSKI, G. **Android hacker's handbook**. [S.l.]: John Wiley & Sons, 2014.

FARIAS, F. P.; BARROS, R. Lgpd – from theory to practice. In: **2022 17th Iberian Conference on Information Systems and Technologies (CISTI)**. [S.l.: s.n.], 2022. p. 1–6.

GCF Global. **Informática Básica - O que é um aplicativo ou um programa?** 2018. Disponível em: <https://edu.gcfglobal.org/pt/informatica-basica/o-que-e-um-aplicativo-ou-um-programa/1>. Acessado em 29 de novembro de 2022.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4a. ed. São Paulo: Atlas, 2002. ISBN 85-224-3169-8.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. [S.l.]: Brasport, 2018.

IBGE. **Uso de Internet, televisão e celular no Brasil**. 2019. Disponível em: <https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celu-lar-no-brasil.html#subtitulo-1>. Acessado em 19 de setembro de 2022.

KASPERSKY. **O que é jailbreak – definição e explicação**. 2023. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-jailbreaking>. Acessado em 4 de janeiro de 2023.

KEMP, S. **DIGITAL 2020: BRAZIL**. 2020. Disponível em: <https://datareportal.com/reports/digital-2020-brazil>. Acessado em 16 de novembro de 2022.

LOPES, P. **PSI – Política de Segurança da Informação**. 2017. Disponível em: <https://periciacomputacional.com/psi-politica-de-seguranca-da-informacao/>. Acessado em 4 de janeiro de 2023.

MEIRELLES, F. S. Pesquisa anual do fgvcia. **Uso da TI–Tecnologia da Informação nas Empresas. Fundação Getúlio Vargas**, 2020.

RAPÔSO, C. F. L.; LIMA, H. M. de; JUNIOR, W. F. de O.; SILVA, P. A. F.; BARROS, E. E. de S. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58–67, 2019.

ROCCIA, R. D. Usuários respeitam as normas de criação de senhas seguras? uma análise de datasets de senhas vazadas. 2021.

SÁ, M. D. de *et al.* Análise do impacto da nova lei de proteção de dados pessoais nas aplicações de internet das coisas: aplicações mobile do governo. Universidade Federal de Minas Gerais, 2019.

STUDY.COM. **Mobile Devices: Examples, Impact Trends**. 2020. Disponível em: <https://study.com/academy/lesson/mobile-devices-examples-impact-trends.html>. Acessado em 29 de novembro de 2022.

WAZLAWICK, R. S. **Metodologia de Pesquisa para Ciência da Computação**. 1a. ed. Rio de Janeiro: Elsevier Editora, 2009. ISBN 978-85-352-3522-7.