INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA, CAMPUS MONTEIRO
DIRETORIA DE DESENVOLVIMENTO E ENSINO
CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FRANCISCO LUCAS DA SILVA CHAVES

SEGURANÇA DE APLICATIVOS MOBILE:

segurança da informação e a privacidade em aplicativos mobile

MONTEIRO

2025

FRANCISCO LUCAS DA SILVA CHAVES

SEGURANÇA DE APLICATIVOS MOBILE:

segurança da informação e a privacidade em aplicativos mobile

Trabalho de Conclusão de Curso apresentado ao Campus Monteiro do Instituto Federal da Paraíba como requisito para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Prof. Gilmar de Jesus Barros

MONTEIRO

2025

Dados Internacionais de Catalogação na Publicação – CIP
Bibliotecária responsável Porcina Formiga dos Santos Salgado CRB15/204 IFPB Campus Monteiro.

C512s Chaves, Francisco Lucas da Silva.
Segurança de aplicativos Mobili:segurança da informação e a privacidade em aplicativos Mobili / Francisco Lucas da Silva Chaves – Monteiro-PB. 2025.
47fls. : il.

TCC (Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas) - Instituto Federal de Educação, Ciência e Tecnologia da Paraíba - IFPB campus, Monteiro.

Orientador: Prof. Gilmar de Jesus Barros.

1. Segurança - Informação 2. Aplicativos Mobili 3. Politicas privacidade. I. Titulo .

CDU 004.056.53

FRANCISCO LUCAS DA SILVA CHAVES

SEGURANÇA DE APLICATIVOS MOBILE:

segurança da informação e a privacidade em aplicativos mobile

Trabalho de Conclusão de Curso apresentado ao Campus Monteiro do Instituto Federal da Paraíba como requisito para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Prof. Gilmar de Jesus Barros

Aprovado em 20 de Março de 2025

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
GILMAR DE JESUS BARROS
Data: 30/03/2025 14:14:25-0300
Verifique em https://validar.iti.gov.br

Prof. Gilmar de Jesus Barros (Orientador)

gov.br Documento assinado digitalmente
GILVONALDO ALVES DA SILVA CAVALCANTI
Data: 30/03/2025 21:22:19-0300
Verifique em https://validar.iti.gov.br

Prof. Gilvonaldo Alves da Silva Cavalcanti (Examinador)

gov.br Documento assinado digitalmente
THALLYTA MARIA MEDEIROS SILVA PEREIRA
Data: 28/03/2025 10:56:07-0300
Verifique em https://validar.iti.gov.br

Profa. Thallyta Maria Medeiros Silva Pereira (Examinador)

RESUMO

O estudo teve o intuito de compreender a segurança dos aplicativos Mobile, levando em consideração seu uso diário e o aumento do uso da internet pela sociedade de modo geral. Desse modo, o objetivo do estudo foi verificar quanto ao cumprimento dos padrões de segurança da informação e à possibilidade de divulgação de dados dos usuários para atividades ilegais. Para isso, foi feita uma pesquisa qualitativa, de cunho bibliográfico, avaliando estudos que analisaram a qualidade e políticas de privacidade voltadas aos aplicativos virtuais presentes para *download*. O estudo buscou responder a seguinte problemática: Os usuários de aplicativos Mobile e da internet estão sendo protegidos pelas Políticas de Privacidade dos aplicativos para *download* e pela Segurança da Informação? Como resultado, foi verificado que nos estudos realizados por Cunha (2022); Martino (2016) e Nascimento (2023), que os aplicativos Mobile de áreas distintas, contam com problemas tanto na Segurança da Informação dos usuários como nas Políticas de Privacidade disponibilizada pelos aplicativos. Sendo assim, concluiu-se que os engenheiros e fundadores dos aplicativos móveis devem trabalhar em conjunto com o usuário para que sua privacidade e suas informações e dados estejam seguros durante o uso desses mecanismos. Os usuários podem passar por um letramento digital, o qual proporcionaria maior conhecimento sobre as ameaças e possíveis ações que os *hackers* possam realizar para ter acesso as informações e dados privados e valiosos deles. Nesse mesmo sentido, os engenheiros e fundadores desses aplicativos devem pensar cuidadosamente nas Políticas de Privacidade disponibilizadas e também devem analisar técnicas capazes de introduzir maior segurança aos usuários.

Palavras-chave: aplicativos Mobile; padrões de segurança; segurança da informação; políticas de Privacidade.

ABSTRACT

The study aimed to understand the security of mobile applications, taking into account their daily use and the increased use of the internet by society in general. Thus, the objective of the study was to verify compliance with information security standards and the possibility of disclosing user data for illegal activities. To this end, a qualitative, bibliographical research was carried out, evaluating studies that analyzed the quality and privacy policies aimed at virtual applications available for download. The study sought to answer the following question: Are users of mobile applications and the internet being protected by the Privacy Policies of the applications for download and by Information Security? As a result, it was found that in the studies carried out by Cunha (2022); Martino (2016) and Nascimento (2023), mobile applications from different areas have problems both in the Information Security of users and in the Privacy Policies made available by the applications. Therefore, it was concluded that mobile application engineers and founders must work together with users to ensure that their privacy and information and data are secure when using these mechanisms. Users can undergo digital literacy, which would provide greater knowledge about the threats and possible actions that hackers can take to gain access to their private and valuable information and data. In the same sense, engineers and founders of these applications must carefully consider the Privacy Policies made available and must also analyze techniques capable of introducing greater security to users.

Keywords: mobile Applications; security standards; information security; privacy Policies.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

A ampla acessibilidade a dispositivos móveis e aplicativos, tanto para entretenimento quanto para trabalho, expõe os usuários a invasões maliciosas. Consequentemente, Graciano (2017) menciona que os dados pessoais e empresariais podem ser facilmente roubados de um dispositivo que, à primeira vista, parece inofensivo.

Essa vulnerabilidade pode levar a falências organizacionais ou exposições pessoais indesejadas. Para garantir a segurança de um aplicativo, Graciano (2017) destaca três fatores essenciais: a infraestrutura técnica, as pessoas envolvidas no desenvolvimento e o próprio aplicativo.

A segurança da informação é um tema recorrente na computação, especialmente devido aos avanços tecnológicos. Entretanto, Graciano (2017) menciona que essa evolução também cria novas oportunidades para invasores, que tentam interceptar dados de navegadores de várias maneiras. Além disso, dispositivos como smartphones, tablets e PDAs tornaram-se alvos frequentes de ataques devido à sua semelhança com computadores e também em razão da facilidade de acesso.

Ademais, no século XX, o desenvolvimento das tecnologias de informação e comunicação (TIC), especialmente a internet, provocou mudanças significativas. De acordo com Cavalcante (2019), a internet facilitou a distribuição global de informações e comunicação. Com base nisso, com um computador conectado à internet, qualquer pessoa pode compartilhar e armazenar informações em escala global, acessando uma vasta gama de conhecimentos.

À medida que a tecnologia se integra, memorandos corporativos foram substituídos por e-mails, enquanto revistas e jornais deram lugar aos blogs, e a música se tornou digital. Segundo Cavalcante (2019), embora esses avanços sejam notáveis, computadores e internet continuam a facilitar tarefas, tornando o poder computacional mais acessível e integrando ferramentas funcionais em *software* e *hardware* para aumentar a eficiência do trabalho.

Apesar disso, Cavalcante (2019) destaca que algumas tendências anteriores ainda persistem na era móvel, tais como o fácil acesso à informação e ao poder computacional. Hoje em dia, empresas e indivíduos se comunicam de maneiras

bastante diferentes, o que permite que os usuários sejam produtivos em qualquer lugar, realizando seu trabalho de forma flexível.

Com a era móvel, a quantidade de informações trocadas aumentou exponencialmente, tornando a segurança da informação uma preocupação constante. Martino (2016) afirma que, à medida que a tecnologia em nuvem avança, ela se expande, especialmente na utilização de serviços, aumentando significativamente a produção e distribuição de informações para diversos fins. Com a internet, qualquer pessoa pode acessar produtos e serviços, especialmente por meio de dispositivos móveis.

Ao estabelecer políticas de privacidade, os usuários podem proteger as informações fornecidas, garantindo quais dados são armazenados e como. Beal (2005) explica que a segurança da informação envolve proteger dados contra ameaças que possam comprometer sua integridade, disponibilidade e confiabilidade.

. Ademais, a questão central a ser investigada é: os usuários de aplicativos móveis e da internet estão realmente protegidos pelas políticas de privacidade e pelas medidas de segurança da informação?

A motivação para este estudo surgiu da preocupação com o número crescente de aplicativos que oferecem serviços e informações de terceiros, sem priorizar a segurança das informações trocadas. O aumento do uso desses dispositivos é evidente, assim, segundo Cunha (2022), em 2019, 42% da população mundial usava redes sociais, totalizando 3,2 bilhões de pessoas. Esse número saltou para 4,62 bilhões em 2022, evidenciando um crescimento acelerado, impulsionado pelos algoritmos que incentivam o uso dos serviços.

Esse fenômeno resulta em horas de consumo de conteúdo, levando os usuários a confiar em outros, que podem divulgar sites de apostas, jogos ou compras, levando à disponibilização de dados pessoais. Casos de perda de contas em redes sociais, como o Instagram, devido ao compartilhamento descuidado de informações pessoais, são cada vez mais comuns.

Assim, avaliar o nível de segurança proporcionado pelos aplicativos móveis é essencial para informar tanto a comunidade acadêmica quanto o público em geral sobre quais podem ser utilizados de forma segura e quais recursos podem aprimorar a segurança virtual durante a navegação por esses mecanismos e nas redes sociais.

O presente trabalho está organizado em três capítulos. A Introdução apresentada oferece uma visão geral do que será analisado na Fundamentação

Teórica, que é o segundo capítulo. Este capítulo contém quatro seções: a primeira aborda o surgimento dos aplicativos móveis, contextualizando sua evolução e importância na sociedade atual.

A segunda seção, intitulada Padrões de Segurança da Informação, aborda a relevância da segurança na era móvel, ao apresentar normas e leis pertinentes. Por outro lado, a terceira seção investiga a aplicação da segurança da informação em aplicativos móveis, destacando tanto os riscos quanto as medidas cabíveis.

A quarta seção, “Qualidade e Políticas de Privacidade dos Aplicativos Móveis”, analisa estudos de segurança e privacidade dessas ferramentas.. O terceiro capítulo, intitulado “Considerações Finais”, apresenta os principais resultados da pesquisa, avaliando se os objetivos foram alcançados e propondo direções para estudos futuros.

2 OBJETIVOS

2.1 OBJETIVOS GERAIS

Analisar a conformidade dos aplicativos com os padrões de segurança e privacidade, bem como identificar os riscos associados ao uso cotidiano dessas tecnologias.

2.2 OBJETIVOS ESPECÍFICOS

- Avaliar a qualidade e as políticas de privacidade dos aplicativos disponíveis para *download*.
- Investigar se os usuários de aplicativos móveis e da internet estão realmente protegidos pelas políticas de privacidade e pelas medidas de segurança da informação.
- Informar a comunidade acadêmica e o público em geral sobre quais aplicativos podem ser utilizados de forma segura e quais recursos podem aprimorar a segurança virtual.

3 METODOLOGIA

Foi realizada uma pesquisa qualitativa, de cunho bibliográfico, a qual avaliou estudos que analisaram a qualidade e as políticas de privacidade dos aplicativos disponíveis para *download*. A crescente utilização de dispositivos móveis conectados à internet trouxe novos desafios de segurança, expondo os usuários a diversas vulnerabilidades. Por essa razão, esse estudo se fez necessário, trazendo conhecimentos pertinentes aos inúmeros usuários desses dispositivos.

De acordo com Minayo (2012), a pesquisa qualitativa é uma abordagem que busca compreender fenômenos complexos a partir da perspectiva dos participantes e do contexto em que estão inseridos. No caso deste estudo, a pesquisa qualitativa de cunho bibliográfico envolve a análise detalhada de textos, artigos e outros materiais acadêmicos que discutem a segurança e privacidade de aplicativos móveis.

Com isso, a pesquisa qualitativa foi feita com base em trabalhos acadêmicos direcionados a segurança de aplicativos mobile, riscos e vulnerabilidades dos usuários nesses aplicativos. Os estudos selecionados foram baseados nos seguintes critérios de inclusão: Estudos que abordem a segurança e privacidade de aplicativos móveis; artigos publicados entre 2010 e 2023; e pesquisas que utilizem metodologias qualitativas.

Além disso, Minayo (2012), a pesquisa qualitativa permite uma compreensão aprofundada dos desafios e soluções relacionadas à segurança da informação em aplicativos móveis, fornecendo percepções valiosas para a comunidade acadêmica e o público em geral.

Desse modo, a pesquisa qualitativa proporciona uma compreensão sobre a infraestrutura técnica, voltada a avaliação das tecnologias e sistemas utilizados para garantir a segurança dos aplicativos, compreendendo a funcionalidade e medidas de segurança implementada aos aplicativos, assim como os riscos associados a vulnerabilidade dos usuários cotidianamente ao utilizar esses aplicativos.

4 REFERENCIAL

4.1 SURGIMENTO DOS APLICATIVOS MOBILE

A ideia de criar um dispositivo que permitisse a comunicação em diferentes locais começou a tomar forma em 1947; no entanto, as limitações tecnológicas da época impediram seu progresso. De acordo com Bine e Kuk (2015), a primeira ligação entre um dispositivo móvel e um telefone fixo ocorreu em 1973, utilizando conceitos previamente desenvolvidos.

Em 1983, a Motorola lançou o DynaTAC 8000x, seu primeiro modelo de celular, contudo, devido ao seu alto custo, ele não se popularizou entre os consumidores. De acordo com Bine e Kuk (2015), essa invenção revolucionária permitiu a comunicação em diversos locais, superando as limitações do ambiente doméstico ou profissional.

Bine e Kuk (2015) afirmam que o avanço do *hardware* e *software* foi crucial para tornar os dispositivos móveis mais atraentes e versáteis. Nesse viés, os primeiros modelos já contavam com memória interna para armazenamento de contatos, cálculo, identificação de chamadas e troca de mensagens de texto, entre outras funcionalidades. Além disso, com o desenvolvimento da internet, surgiram telas coloridas e a capacidade de reproduzir músicas.

Os smartphones, sendo dispositivos pequenos e portáteis, possuem mais poder de processamento do que a maioria dos computadores, além disso, esses dispositivos permitem tanto a instalação quanto a desinstalação de aplicativos. Segundo Bine e Kuk (2015), o crescimento dessa nova categoria deve-se à popularidade dos laptops e dispositivos portáteis na década de 90, muitos dos quais eram capazes de rodar o Microsoft Disk Operating System (MS-DOS) e permitiam a instalação de software específico.

De acordo com Morimoto (2009), a mobilidade refere-se aos principais dispositivos emergentes no mercado global, englobando sistemas que podem ser facilmente transportados ou que operam mesmo em movimento. Para um dispositivo ser considerado móvel, ele deve possuir características como tamanho compacto, baixo consumo de energia, memória adequada, capacidade de processamento de dados e monitoramento de nível de potência para evitar perda de informações.

Fling (2009) destaca que é essencial que um dispositivo móvel possa realizar tarefas por meio de textos, áudios e vídeos, além de ter acesso à internet. Características únicas que o diferenciam de outros dispositivos incluem ser pessoal, fornecer informações em tempo real, ser facilmente transportável e integrar canais

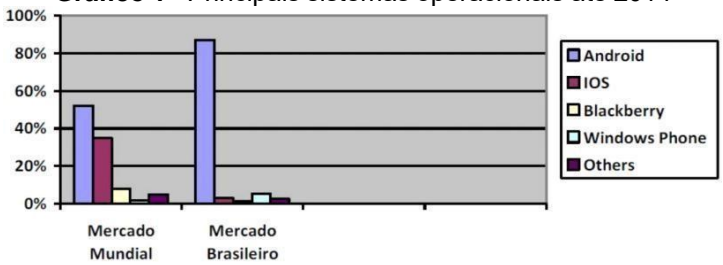
de pagamento, além de estar presente em momentos de impulso criativo.

Além disso, Bine e Kuk (2015) observam que a transmissão nos primeiros modelos de dispositivos móveis era realizada por meio de um sistema analógico de voz. Posteriormente, esse sistema evoluiu para meios digitais, como o Code Division Multiple Access (CDMA) e o Global System for Mobile Communications (GSM), esses avanços tecnológicos deram origem a diferentes gerações de dispositivos móveis, incluindo 2G, 3G e 4G, sendo o 4G o mais amplamente utilizado nos dispositivos modernos.

Com esses dispositivos, os usuários têm acesso a informações de qualquer lugar de maneira rápida e fácil, o que torna a computação móvel responsável pelo surgimento da quarta revolução na computação. Além disso, Bine e Kuk (2015) mencionam que o aumento da potência dos computadores, aliado a novos formatos e programas simples, tornou o uso dessa tecnologia cada vez mais indispensável na contemporaneidade.

Conforme Bine e Kuk (2015), o sistema operacional, além de gerenciar o hardware e o software do dispositivo, interage diretamente com o usuário. Dessa forma, várias empresas de tecnologia desenvolveram plataformas para atender às necessidades dos dispositivos móveis. Atualmente, três sistemas operacionais se destacam no Brasil e no exterior. O Gráfico 1, elaborado com dados de maio de 2014, ilustra essa situação.

Gráfico 1 - Principais sistemas operacionais até 2014



Fonte: Bine e Kuk (2015, p. 4)

É possível constatar que o Android, que é baseado no sistema Linux, lidera o mercado no Brasil, assim como diversos outros países. De acordo com Bine e Kuk (2015), essa popularidade se deve, sobretudo, à facilidade de uso e ao baixo custo. Além disso, os aplicativos geralmente precisam ser desenvolvidos especificamente para cada sistema operacional, devido às suas características distintas

4.2 PADRÕES DE SEGURANÇA DA INFORMAÇÃO

Os aplicativos conseguem ajustar-se ao perfil do usuário, oferecendo serviços personalizados conforme suas preferências. Para isso, é necessário coletar dados que, se identificáveis, são considerados dados pessoais (Silva *et al.*, 2018). Silva *et al.* (2018) afirmam que a coleta de dados pessoais por sites e aplicativos móveis tem crescido significativamente, com muitas empresas utilizando essas informações como fonte de renda, incluindo agências de publicidade que os coletam para fins publicitários.

Silva *et al.* (2018) destaca que devido à crescente facilidade de uso de ferramentas como a Inteligência Artificial (IA), os aplicativos coletam dados dos usuários, incluindo padrões de uso, funções mais solicitadas e histórico de navegação na internet. Consequentemente, a maioria dos aplicativos populares possui a capacidade de capturar e analisar esses dados.

Os aplicativos móveis apresentam maiores riscos de privacidade do que a navegação em desktops. Por exemplo, os “cookies”, principais meios de autenticação na internet, podem ser facilmente excluídos para proteger a privacidade. No entanto, os smartphones têm dificuldade em mudar de identidade, o que representa um desafio à autenticação. Silva *et al.* (2018) explicam que os dados presentes em computadores podem ser compartilhados entre vários usuários, enquanto os smartphones geralmente são usados por uma única pessoa, resultando em que a maioria dos dados registrados no dispositivo é gerada pelo mesmo usuário.

A análise das Políticas de Privacidade é crucial no que diz respeito ao uso de dados em aplicativos. Silva *et al.* (2018) destacam que, por meio dessa análise, as empresas podem determinar quais dados são relevantes, o que é compartilhado com terceiros e se os dados estão realmente sendo utilizados para os fins propostos.

Garantir a segurança dos registros em rede tornou-se fundamental, não apenas para *download* ou armazenamento, mas também para proteção contra uso indevido (MARTINO, 2016). O dicionário eletrônico “Houaiss” define segurança como o estado, qualidade ou condição de uma pessoa ou coisa livre de perigos, incertezas e riscos. Assim, a segurança deve ser vista como um estado ou condição criada em um ambiente específico, utilizando medidas apropriadas para garantir a realização segura das atividades.

A definição de conhecimento, segundo Martino (2016), é vaga e varia conforme o contexto, cultura e ciência. No entanto, considera-se que o conhecimento é composto por dados e componentes informacionais; ou seja, dados geram informações, que por sua vez geram conhecimento. Na teoria da informação, os dados consistem em mensagens sobre eventos ou fenômenos, organizados em coleções.

A ISO/IEC 27002:2008 trata-se de uma regulamentação global que define orientações para a segurança de dados em dispositivos móveis, sendo crucial para assegurar a integridade e a confidencialidade das informações manipuladas em aplicativos. Ela define Segurança da Informação como a proteção da informação contra diversas ameaças, garantindo a continuidade dos negócios, minimizando perdas comerciais e maximizando o retorno sobre o investimento. Segundo Beal (2005), essa segurança envolve proteger os dados do usuário, assegurando sua integridade, disponibilidade e confidencialidade.

Ademais, o seu propósito não deve ser visto apenas como “manter todas as informações em segurança”, mas sim como criar políticas eficazes para evitar riscos e vulnerabilidades. Martino (2016) menciona a Lei Carolina Dieckmann (Lei 12.737, de 30 de novembro de 2012), que estabelece que o crime no Código Penal Brasileiro consiste em atacar o sistema de informática de outra pessoa, conectado ou não a uma rede.

Assim, ocorre com a violação desnecessária de mecanismos de segurança, com a intenção de obter, interferir ou destruir dados ou informações sem autorização, visando ganho ilícito. Segundo Martino (2016), a pena prevista é de três meses a um ano de detenção.

Desde 1940, a Associação Brasileira de Normas Técnicas (ABNT) é responsável pelo desenvolvimento de regulamentos e normas técnicas. Segundo Martino (2016), a ABNT (2015) destaca que:

> A normalização é o processo de formulação e aplicação de regras para a solução ou prevenção de problemas, com a cooperação de todos os interessados, e, em particular, para a promoção da economia global. No estabelecimento dessas regras recorre-se à tecnologia como o instrumento para estabelecer, de forma objetiva e neutra, as condições que possibilitem que o produto, projeto, processo, sistema, pessoa, bem ou serviço atendam às finalidades a que se destinam, sem se esquecer dos aspectos de segurança (ABNT, 2015 *apud* Martino, 2016, p. 18).

Desde 2007, a ISO/IEC 17799 foi incorporada à ISO/IEC 27002, estabelecendo um conjunto de práticas para a gestão da Segurança da Informação. Esta norma serve como base para o desenvolvimento de princípios e diretrizes nesse campo.

Gerenciar riscos por meio de políticas, procedimentos, instruções e estruturas organizacionais, sejam elas administrativas, técnicas ou físicas, é essencial para a implementação da ISO/IEC 27002. Martino (2016) define controle como qualquer método utilizado para mitigar fraquezas ou vulnerabilidades de um ativo, seja ele tecnológico, humano, de processo ou ambiental.

A ISO/IEC 27002 abrange 11 categorias de gestão de segurança da informação, conforme listado a seguir:

> Políticas de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gerenciamento das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes de segurança da informação; gestão de continuidade de negócio; conformidade. (Martino, 2016, p. 18 e 19).

Além de estabelecer uma política de segurança da informação, a ISO 27002:2008 também trata da proteção de dados e do controle de acesso, assegurando a integridade e segurança das informações. Termos como Política de Privacidade ou Termos de Privacidade são comumente utilizados quando um usuário acessa ou se registra em um site, garantindo que a empresa informe os usuários sobre como seus dados serão utilizados.

Martino (2016) destaca que a Microsoft, uma das líderes no setor de software, recomenda que todos os sites ou empresas disponibilizem termos e políticas de uso de dados aos usuários. Esses documentos devem abordar aspectos como compartilhamento de informações, esclarecimento de dúvidas sobre cadastro e uso de “cookies”, demonstrando um compromisso com a privacidade dos clientes.

Os termos e condições de um site constituem um contrato entre o site e o usuário. Ao aceitar os termos de serviço, o usuário concorda com todas as cláusulas do documento, que muitas vezes não é lido ou compreendido. Mesmo quando lido, a compreensão pode ser dificultada pela extensão e pelo uso excessivo de termos técnicos (Martino, 2016).

Uma política de privacidade bem elaborada pode atrair visitantes, proporcionando confiança ao explicar o destino dos dados fornecidos. A Microsoft oferece várias recomendações para a criação de uma política de privacidade eficaz em sites no Brasil:

> O primeiro passo ao conceber uma política de privacidade eficiente e detalhada é revisar quais parâmetros de privacidade já podem estar em vigor. Verifique que tipo de dados você recebe, como eles são recolhidos, onde são armazenados e outros elementos pertinentes a informações pessoais.
> Determine antecipadamente qual a legislação aplicável. O que você vai incluir na sua política de privacidade pode não depender só de você. Assim como aumentou a preocupação das pessoas com a privacidade, também aumentou a regulamentação formal por parte do governo determinando que elementos certas políticas de privacidade precisam conter.
> Informe explicitamente aos clientes como você usará as informações deles. Lide com aqueles problemas que você não é obrigado a mencionar mas é do seu interesse levantar.
> Peça a um advogado ou especialista em privacidade, se necessário, para redigir ou revisar sua política. Já tendo a noção do que você quer incluir "e o que legalmente deve ser incluído" numa política de privacidade, comece a pôr tudo no papel. Você pode tentar redigir uma política de privacidade por si próprio. Se você fizer isso, é bom que um advogado ou especialista em assuntos de privacidade revise tudo para descobrir eventuais furos. Do mesmo modo, você pode delegar a tarefa a um advogado ou especialista em privacidade.
> Não se esqueça dos empregados em sua política de privacidade. Para muitos, políticas de privacidade destinam-se exclusivamente a usuários e clientes. Mas pode ser importante ter também parâmetros escritos sobre como usar as informações pessoais de seus empregados. Algumas empresas preferem construir parâmetros de privacidade de empregados no mesmo documento que trata dos clientes.
> Nomeie um funcionário para supervisionar a privacidade de forma permanente. A privacidade é um problema de muita relevância. E isso, por sua vez, exige atenção permanente da sua parte. Se a sua empresa tem uma equipe pequena, isso significa acrescentar a privacidade às responsabilidades já existentes de um funcionário.
> Seja coerente com o seu próprio discurso. Um elemento final de uma política de privacidade eficiente é mais importante que o papel em que é escrita. Se e quando você tem uma política em vigor, mova céus e terras para garantir que seus empregados a sigam à risca. De novo, um funcionário encarregado só da privacidade pode facilitar essa tarefa. (Martino, 2016, p. 19 e 20).

Cavalcante (2019) também aponta que a discussão sobre Segurança da Informação pode ser realizada de maneira eficaz por meio de modelos, levando em conta três aspectos: disponibilidade, integridade e confidencialidade.

> • Disponibilidade: propriedade a qual mantém as informações acessíveis e utilizáveis em todos os momentos por aqueles que precisam acessá-las.

> • Integridade: propriedade a qual trata de manter as informações na forma em que elas foram usadas. Os dados não podem ser modificadas, removidas ou adicionais por uma parte não autorizadas.
> • Confidencialidade: propriedade que ajuda a proteger adequadamente as informações e recursos de forma confidencial ou sensíveis. Em outras palavras, há uma restrição de acesso aos dados somente aos usuários que estão autorizados a usá-los. (Cavalcante, 2019, p. 28).

Para aprofundar a compreensão sobre Segurança da Informação, Graciano (2017) explora três aspectos fundamentais. A disponibilidade da informação deve ser assegurada para todos que têm autoridade para modificá-la quando necessário, pois o acesso à informação é frequentemente alvo de ataques.

Além disso, Graciano (2017) explica que os cibercriminosos podem, por exemplo, realizar ataques de negação de serviço para impedir que usuários realizem operações bancárias, exigindo pagamento para reverter o ataque. Portanto, medidas como proteções físicas e redundâncias são essenciais para manter a disponibilidade.

Quanto à integridade, Graciano (2017) destaca a importância de garantir que dados e mensagens não sejam alterados durante a transmissão. A integridade pode ser comprometida de várias maneiras, muitas vezes de forma não intencional. Para assegurar a integridade, é crucial que os sistemas implementem backups, auditorias e correções de código.

Finalmente, Graciano (2017) discute a confidencialidade, que garante que apenas pessoas autorizadas tenham acesso à informação. Isso inclui prevenir a divulgação não autorizada e assegurar que dados sensíveis sejam acessados somente por indivíduos com permissão. Medidas como criptografia, controle de acesso, autenticação e segurança física são empregadas para garantir a privacidade dos dados.

4.3 CUMPRIMENTO DOS PADRÕES DE SEGURANÇA DA INFORMAÇÃO NOS APLICATIVOS MOBILE

É fundamental que fornecedores e desenvolvedores de software levem em conta as ameaças à segurança em seus projetos, considerando-as ferramentas essenciais para a proteção de suas empresas. Conforme Batori (2012), a segurança de uma aplicação depende de três fatores: a infraestrutura técnica, os fatores humanos e a própria aplicação.

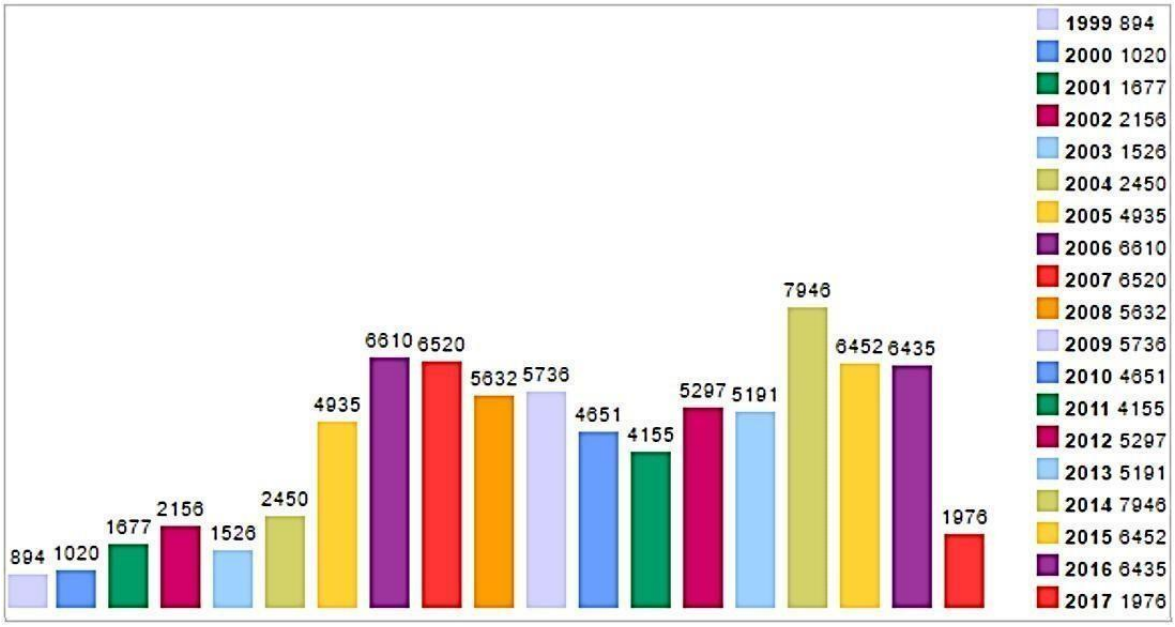
Contudo, a segurança de um software não pode ser facilmente mensurada, diferentemente de outros requisitos, como desempenho, taxa de erros e experiência do usuário. Lipner e Howard (2005), engenheiros de segurança da Microsoft, afirmam que a criação de software altamente seguro envolve três elementos principais: processos repetíveis, treinamento de desenvolvedores ou engenheiros, e dados de métricas e responsabilidades.

Kiyoshi (2012) complementa essa perspectiva, ressaltando que a chave para atender às demandas atuais de segurança está no uso de processos repetitivos, o que facilita a medição, avaliação e minimização de vulnerabilidades no design, codificação e documentação.

Segundo Graciano (2017), é impossível garantir que um aplicativo móvel seja completamente seguro. À medida que novas tecnologias surgem para aprimorar os aplicativos, novos riscos também emergem, afetando milhares de aplicações simultaneamente.

A Figura 1 ilustra as vulnerabilidades documentadas desde 1999 pelo Common Vulnerabilities and Exposures (CVE):

Figura 1 - Vulnerabilidade por ano



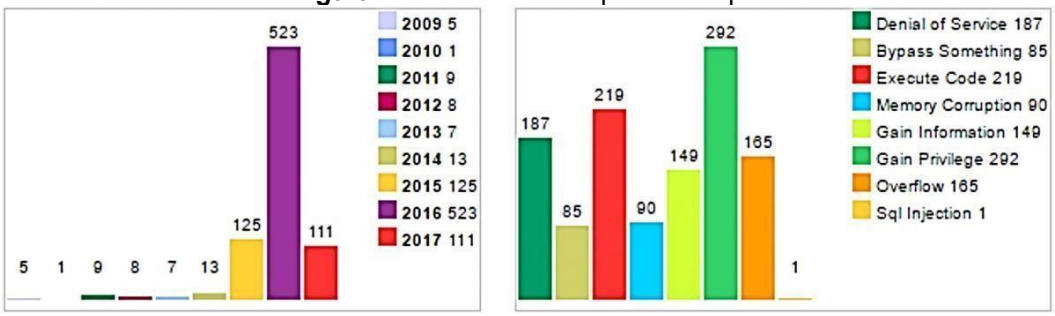
Fonte: Graciano (2017, p. 6)

Como é possível observar na Figura 1, milhares de vulnerabilidades são descobertas todos os anos e, independentemente de quando são descobertas, requerem atenção especial. Muitos desses riscos dependem do desenvolvimento de

um aplicativo seguro para evitar o aparecimento de bugs legados no *software* atual. Sendo assim, os números apresentados são cumulativos.

A Figura 2 exibe dois gráficos que ilustram a quantidade de vulnerabilidades identificadas desde 2009, classificadas em categorias como Denial of Service (DoS) e SQL Injection. Desde aquele ano, foram registradas 1.976 vulnerabilidades, das quais 5,61% são específicas do Android.

Figura 2 - Vulnerabilidade por ano e tipo



Fonte: Graciano (2017, p. 7)

A proteção é essencial, independentemente da plataforma. Aplicativos móveis que acessam a internet para realizar tarefas estão expostos a ataques tanto no lado do cliente quanto no servidor, oferecendo oportunidades para invasores.

Leavitt (2011), presidente da Leavitt Communications, destaca que quanto mais a tecnologia é utilizada, maior é sua exposição a *hackers*. Isso é particularmente alarmante no contexto da tecnologia móvel, dado o aumento global de dispositivos em uso e o crescimento no *download* de aplicativos sem a devida verificação de segurança.

Em virtude do uso crescente de aplicativos móveis para transações, como pagamentos e acesso a contas bancárias, Graciano (2017) explica que os criminosos encontram, constantemente, alvos fáceis, como pessoas analfabetas, idosos ou adolescentes.

Além disso, Graciano (2017) destaca que esses ataques são facilitados pela conexão contínua dos aplicativos à internet. Em razão disso, empresas como a McAfee, monitoram mais de 55 mil novos *malwares* diariamente, buscando reduzir os golpes que ocorrem diariamente com pessoas que não sabem usar de forma segura os aplicativos.

Nesse sentido, o Open Web Application Security Project[1] (OWASP) identificou, em um estudo de 2014, dez principais categorias de risco em aplicativos móveis. Em seguida, são descritos os dez principais riscos:

> 1. Comunicação fraca com o servidor: Servidores que fornecem APIs inseguras são vulneráveis a ataques que manipulam dados transmitidos entre dispositivos e servidores.
> 2. Armazenamento inseguro de dados: A maioria das violações de segurança ocorre porque os desenvolvedores subestimam a capacidade de malwares acessarem o sistema de arquivos dos dispositivos.
> 3. Proteção insuficiente na camada de transporte: Falta de criptografia adequada durante a comunicação com o servidor, permitindo que invasores monitorem informações transmitidas.
> 4. Vazamento de dados indesejados: Dados sensíveis armazenados em locais acessíveis no dispositivo podem ser explorados por outros aplicativos ou manuseados indevidamente.
> 5. Fraca autorização e autenticação: A ausência de mecanismos robustos de autenticação permite que invasores realizem operações não autorizadas.
> 6. Criptografia quebrada: Exploração de criptografia comprometida por meio de vulnerabilidades de código ou ataques de força bruta.
> 7. Injeções no lado cliente: Códigos maliciosos são executados no aplicativo devido ao processamento inadequado de dados, o que pode resultar em danos significativos.
> 8. Segurança baseada em inputs inseguros: Entradas de dados não validadas tornam os sistemas vulneráveis a ataques, como interceptação de formulários e execução de comandos maliciosos.
> 9. Tratamento impróprio de sessões: Falhas no gerenciamento de sessões podem permitir que invasores falsifiquem autenticações e obtenham acesso não autorizado.
> 10. Falta de proteção binária: Sem proteção do código binário, o software fica vulnerável à engenharia reversa e modificações por invasores. (Graciano, 2017, p. 10).

Além do exposto, a Tabela 1 a seguir exibe uma avaliação de risco fundamentada nos dados da OWASP, ressaltando os níveis de exploração, prevalência, detectabilidade e impacto dos riscos.

[1] OWASP: É uma organização sem fins lucrativos com foco em melhorar a segurança no ambiente digital.

Tabela 1 - Análise de riscos por meio dos dados da OWASP

Descrição	Exploração	Prevalência	Detectabilidade	Impacto
Comunicação fraca com Servidor	Fácil	Comum	Média	Severo
Armazenamento inseguro de dados	Fácil	Comum	Fácil	Severo
Proteção Insuficiente na camada de transporte	Difícil	Comum	Fácil	Moderado
Vazamento de dados indesejados	Fácil	Comum	Fácil	Severo
Fraca autorização e autenticação	Fácil	Comum	Fácil	Severo
Criptografia quebrada	Fácil	Comum	Fácil	Severo
Injeções no lado cliente	Fácil	Comum	Fácil	Moderado
Decisões de segurança baseados em inputs inseguros	Fácil	Comum	Fácil	Severo
Tratamento impróprio de sessões	Fácil	Comum	Fácil	Severo
Falta de proteção binária	Media	Comum	Fácil	Severo

Fonte: Graciano (2017, p. 13)

Para reduzir as ameaças à segurança em aplicativos móveis, Cavalcante (2019) recomenda a implementação de Políticas de Segurança da Informação (PSI), que estabelecem diretrizes e procedimentos para assegurar o uso seguro dos recursos de TI nas organizações. Essas políticas visam proteger a organização e seus funcionários contra a perda ou uso indevido de informações, garantindo a integridade e disponibilidade dos dados.

Cavalcante (2019) também enfatiza a importância da notificação de incidentes e abusos, além de mecanismos de autenticação robustos (como senhas complexas e biometria), criptografia, backups e logs para a proteção dos dispositivos. Ferramentas como *antimalware*, *firewalls* e filtros de e-mail também são cruciais na defesa contra ameaças externas.

Adicionalmente, Cavalcante (2019) ressalta a relevância do teste de reputação de sites, que avalia a segurança de um site com base em sua reputação, e dos programas de verificação de vulnerabilidades, que identificam e minimizam riscos nos sistemas. Esses mecanismos são essenciais para proteger infraestruturas digitais e garantir que sistemas e aplicativos estejam seguros contra ataques maliciosos.

Por fim, Cavalcante (2019) desenvolveu um Guia de Segurança da Informação em Dispositivos Móveis, focado no ambiente corporativo, destacando que os dados armazenados em dispositivos empresariais estão suscetíveis a perda,

roubo ou uso indevido, exigindo políticas de proteção mais abrangentes que incluam tanto os dispositivos quanto os aplicativos e dados corporativos.

5 ANÁLISE DE DADOS

Nas seções anteriores, foram apresentadas informações essenciais para compreender o desenvolvimento dos aplicativos móveis, além de aspectos e considerações sobre Segurança da Informação e Políticas de Privacidade. Em razão disso, essa seção se dedica a analisar estudos anteriores que investigam se os usuários desses dispositivos e da internet, estão sendo adequadamente protegidos na realização de *download*.

Primeiramente, destacamos o estudo de Costa (2022), que avaliou critérios de segurança e privacidade de 30 aplicativos móveis desenvolvidos pelo governo brasileiro, totalizando mais de 935 milhões de *downloads* na Google Play Store.

Em maio de 2021, foi constatado que o governo brasileiro disponibilizava até então 150 aplicativos móveis em sua conta na Google Play Store. Além disso, Costa (2022, p. 17) verificou que:

> O Governo do Brasil disponibiliza aplicativos de diferentes segmentos e áreas de governo, como na área de Previdência Social (“Meu INSS”), na área de Renda e Tributação (“Meu Imposto de Renda”), na área de Educação (“ENEM”), na área de Saúde (“Conecte SUS”), na área de Segurança Pública (“Sinesp Cidadão”), entre outras. (Costa, 2022, p. 17).

Ao longo do período analisado, os aplicativos do Governo Federal foram baixados mais de 267 milhões de vezes, além de terem recebido mais de 85 milhões de atualizações. Ademais, Costa (2022) menciona a criação de uma conta na Google Play Store para o “Governo do Brasil”, no qual essas ferramentas estão disponíveis.

Segundo Matos Neto (2020), a Portaria nº 39, de 9 de julho de 2019, do Ministério da Economia, regulamenta o envio simultâneo de aplicativos do Governo Federal em lojas desses mecanismos por meio de uma única conta editorial, que deve incluir todos os registros dos órgãos governamentais brasileiros.

É essencial que os cidadãos possam acessar os aplicativos oficiais através de uma conta única do Governo Federal, facilitando sua localização. Além disso, foi observado que cerca de 43 órgãos públicos já possuíam contas de desenvolvedores

de aplicativos antes da centralização. Desse modo, centralizar desses mecanismos em uma única conta também aumentaria a segurança dos usuários (Matos Neto, 2020).

Durante a pesquisa, Costa (2022) constatou que documentos jurídicos brasileiros passaram a ser acessíveis digitalmente por meio de aplicativos, tais como Cadastro de Pessoas Físicas (CPF), Carteira Nacional de Habilitação (CNH), Carteira de Trabalho e Título de Eleitor, mantendo a validade dos documentos físicos.

Além disso, outro exemplo é o Certificado de Registro e Licenciamento de Veículos (CRLV), antigamente disponível apenas na versão impresso. Segundo Costa (2022), atualmente ele passou a existir em sua versão eletrônica, no aplicativo "Carteira Digital de Trânsito", a partir de 6 de setembro de 2020.

A pandemia da Covid-19 também contribuiu para tornar o smartphone uma ferramenta indispensável de acesso aos serviços governamentais. O "Auxílio Emergencial", por exemplo, foi totalmente digitalizado pelo governo brasileiro, oferecendo proteção emergencial durante a crise financeira e sanitária sem precedentes causada pela pandemia do novo Coronavírus (Costa, 2022).

Assim, Costa (2022) destaca que, por meio do aplicativo "CAIXA Tem", o cidadão pode cadastrar seu CPF, acompanhar a situação de aprovação e receber automaticamente o valor do auxílio em sua conta no aplicativo móvel. Além disso, os beneficiários também podem utilizar cartões de débito virtuais para realizar pagamentos e compras sem precisar ir a uma agência bancária.

Costa (2022) observou que as iniciativas do Governo Móvel possuem duas modalidades, conforme a Tabela 2 a seguir:

Tabela 2 - Duas dimensões das iniciativas do Governo Móvel

	INDIVIDUAL	ORGANIZAÇÃO
USO INTERNO	Governo Móvel para Servidores (mG2E) Refere-se ao uso das tecnologias móveis por parte de servidores públicos ou funcionários a serviços do governo	Governo Móvel para Governos (mG2G) Refere-se ao uso das tecnologias móveis para aprimorar a interação entre agências governamentais
USO EXTERNO	Governo Móvel para Cidadão (mG2C) Aprimoramento da interação entre instituições públicas e cidadão por meio das tecnologias móveis	Governo Móvel para Empresas (mG2B) Uso das tecnologias móveis para melhorar a interação entre instituições públicas e organizações do setor privado

Fonte: Costa (2022, p. 16)

Segundo o relatório de 2015 do IBM Center for The Business of Government[2], a classificação anterior pode ser separada em dois grupos, conforme detalhado na Tabela 3. Costa (2022) afirma que o primeiro tipo de aplicativo é direcionado para uso interno das instituições públicas, permitindo que os funcionários das agências governamentais desempenhem suas funções de maneira mais eficiente.

Os aplicativos voltados para os cidadãos compõem o segundo grupo, possibilitando o acesso aos serviços governamentais por qualquer pessoa. Conforme Costa (2022), a finalidade desse grupo é empregar novas tecnologias para melhorar a interação entre a sociedade e a administração pública.

Tabela 3 - Aplicativos Mobile governamentais

USO INTERNO	Voltado a própria Instituição (melhoria da produtividade dos órgãos)
USO EXTERNO	Voltado ao Cidadão (aprimorar a relação dos órgãos com a sociedade)

Fonte: Costa (2022, p. 16)

Com base nos tipos de aplicativos móveis disponibilizados pelo Governo Móvel, Costa (2022) acredita que sua pesquisa oferecerá uma análise sobre a segurança e privacidade dessas ferramentas destinados ao uso público, ou seja, acessíveis a qualquer pessoa interessada em utilizar o serviço móvel do governo brasileiro.

Além disso, Costa (2022) identificou dez principais riscos nos aplicativos móveis, bem como alguns comportamentos dos usuários que podem comprometer a segurança. Após essa explicação, ele apresenta o modelo de ameaças utilizado na pesquisa. O objetivo da modelagem de ameaças é identificar e avaliar vulnerabilidades que podem afetar os recursos, ou seja, verificar o que pode dar errado em um aplicativo móvel.

De acordo com Tarandach e Coles (2020), a modelagem de ameaças envolve a análise de um sistema para detectar vulnerabilidades decorrentes de escolhas inadequadas de design. Segundo Costa (2022), durante essa modelagem, um aplicativo móvel é visto como uma coleção de seus componentes e suas interações

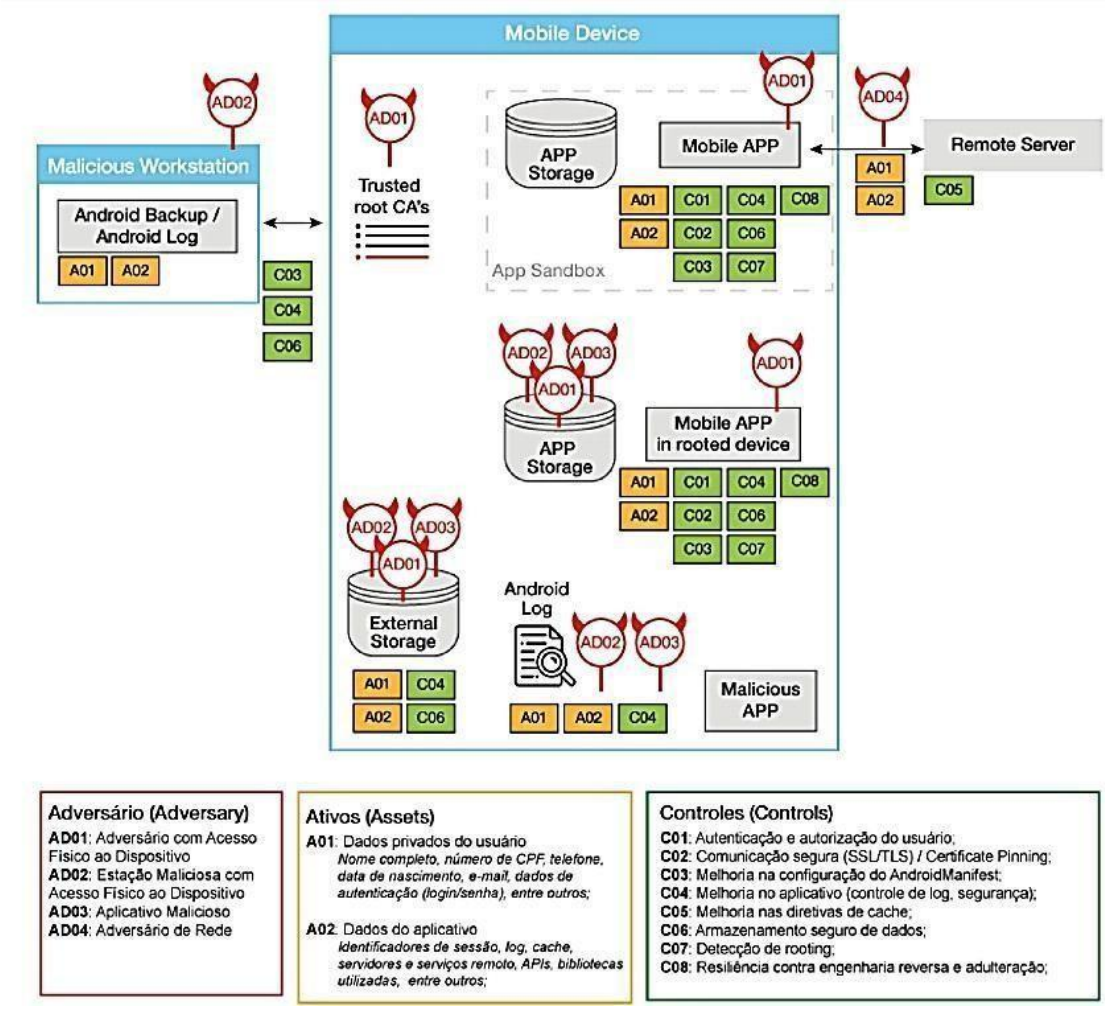
[2] IBM CENTER: É um centro de pesquisa que estuda e promove melhores práticas para administração pública.

com o ambiente externo. O objetivo é descobrir como essas partes podem falhar ou o que pode levá-las a falhar.

Há diversos métodos de modelagem de ameaças, como STRIDE, PASTA e Trike. Contudo, conforme Tarandach e Coles (2020), nenhum método se sobressai aos demais, visto que para certas organizações, equipes, tecnologias ou exigências de conformidade, uma abordagem pode ser mais eficiente do que outra.

Assim, Costa (2022) explica que utilizou o modelo de ameaças baseado na descoberta de ameaças desenvolvido por Kesäniemi e Mäkelä (2011), que realiza cinco perguntas iniciais: 1. O que queremos proteger e por quê? 2. Onde o ataque poderia acontecer? 3. O que poderia dar errado? 4. Temos proteção adequada? 5. Qual é o risco que aceitamos?

Figura 3 - Diagrama do modelo de ameaças dos aplicativos Mobile analisados



Fonte: Costa (2022, p. 26)

Além disso, Costa (2022) explica que existem diferentes formas de realizar testes em aplicativos móveis. Os mais comuns são:

> - **Teste caixa-preta -** é conduzido sem que o testador tenha qualquer informação sobre o aplicativo que está sendo testado. Esse processo às vezes é chamado de “teste de conhecimento zero”. O objetivo principal desse teste é permitir que o testador se comporte como um adversário real.
> - **Teste caixa-branca -** é o oposto do teste caixa-preta, no sentido de que o testador tem total conhecimento do aplicativo. Às vezes é chamado de “teste de conhecimento total”. O conhecimento pode incluir código-fonte, documentação e diagramas, permitindo que o testador construa casos de teste mais sofisticados e granulares.
> - **Teste caixa-cinza -** é todo o teste que se enquadra entre os dois tipos de teste anteriores. Algumas informações são fornecidas ao testador e outras devem ser descobertas. (Costa, 2022, p. 29 e 30).

Costa (2022) aplicou o teste de caixa-preta em sua pesquisa, simulando o comportamento de um possível adversário. No entanto, esses testes podem se aproximar dos de caixa-cinza, pois é preciso desmontar a aplicação para examinar seu interior. Contudo, essa desmontagem não resulta no código-fonte original do aplicativo, o que os distingue dos testes de caixa-branca.

A segurança da aplicação também pode ser avaliada através de análises estáticas (manuais ou automatizadas) e dinâmicas. Essas análises são descritas da seguinte maneira:

> - **Análise estática manual -** é o processo de revisão manual do código-fonte do aplicativo (original ou aproximado, decorrente de uma descompilação). A revisão manual pode ser lenta, tediosa e complexa, especialmente se houver o uso de muitas APIs de terceiros e se forem utilizadas técnicas de ofuscação de código.
> - **Análise estática automatizada -** ferramentas de análise automatizadas podem ser usadas para acelerar o processo de detecção de vulnerabilidades em aplicativos. Essas ferramentas geralmente usam abordagens baseadas em um conjunto predefinido de regras ou práticas recomendadas e, em seguida, normalmente exibem uma lista de descobertas ou avisos para todas as violações detectadas.
> - **Análise dinâmica -** é a avaliação de um aplicativo por meio de sua execução e observação do seu comportamento. É comumente utilizada para verificar dados em trânsito e problemas de configuração no servidor. (Costa, 2022, p. 30).

Desse modo, Costa (2022) constatou que evitou utilizar ferramentas automatizadas na análise de vulnerabilidades, devido às suas limitações, as quais podem resultar em uma alta incidência de falsos positivos. Em vez disso, ele adotou

uma combinação de análise estática (manual e automatizada) e análise dinâmica. Observou-se que:

> Para a análise estática automatizada foram desenvolvidos pelo próprio pesquisador scripts de automatização de algumas atividades recorrentes. A inspeção manual foi utilizada como forma complementar à análise automatizada. A análise dinâmica foi empregada principalmente para observar a comunicação entre os aplicativos móveis e servidores remotos. (Costa, 2022, p. 31).

Durante a análise realizada, foram pontuados critérios de segurança e privacidade, os quais podem ser observados na Tabela 4 a seguir:

Tabela 4 - Critérios avaliados na segurança e privacidade dos aplicativos Mobile do Governo Móvel

Categoria	Critério avaliado	Risco OWASP
Arquivo de Manifesto	AM1: O atributo `allowBackup` está configurado de forma apropriada, não permitindo o backup de dados sensíveis	M2
	AM2: O atributo `debuggable` está configurado de forma apropriada para um aplicativo em versão de produção (não *debuggable*).	M7
	AM3: O atributo `usesCleartextTraffic` está configurado de forma apropriada, não permitindo que o aplicativo e bibliotecas de terceiros trafeguem dados de forma insegura	M3
mazenamento de Dados	AD1: O aplicativo armazena dados sensíveis localmente de forma segura	M2
	AD2: O aplicativo não armazena dados sensíveis em arquivos de cache	M2
	AD3: O aplicativo não registra dados sensíveis em arquivos de *log* ou no *log* do sistema operacional	M2
	AD4: O aplicativo adota proteção contra a captura de dados sensíveis em auto-screenshots, quando o aplicativo é colocado em segundo plano	M2
Transmissão de Dados	TD1: O aplicativo trafega dados em um canal de comunicação de rede seguro (criptografado)	M3
	TD2: O aplicativo adota medida de proteção da comunicação de rede por *SSL Pinning*	M3
Permissões Perigosas	PP: O aplicativo não solicita permissões perigosas além do mínimo necessário	M1
Outros Riscos	OR1: O aplicativo não compartilha dados com terceiros (ex. *Google Firebase*)	M2
	OR2: O aplicativo não utiliza rastreadores (*trackers*) que podem comprometer a privacidade do usuário	M2
	OR3: O aplicativo adota medidas para detectar e responder adequadamente a um dispositivo *rooted*	M8
	OR4: O aplicativo exige a autenticação do usuário a cada novo acesso ao aplicativo (não adota autenticação persistente)	M4

Fonte: Costa (2022, p. 38)

Esta pesquisa indica que a Administração Pública Federal precisa evoluir para garantir a segurança e a privacidade dos usuários dos aplicativos móveis governamentais. Além disso, conforme o Guia de Requisitos Mínimos de Segurança e Privacidade, dados privados e chaves privadas nunca devem ser armazenados em um ambiente à prova de falsificação fornecido pelo fabricante da plataforma, a menos que estejam criptografados e anonimizados, se possível.

Costa (2022) aponta que, em 86% dos aplicativos analisados, os dados privados foram armazenados de maneira insegura. Além disso, foi sugerido que o usuário desative o plano de fundo ou utilize uma tela esmaecida quando o aplicativo for para o plano de fundo, nos campos onde capturas de tela são salvas no armazenamento local; contudo, nenhum aplicativo implementou proteção contra a exposição de dados sensíveis por meio de capturas automáticas de tela.

De acordo com o guia, o usuário deve considerar bloquear o acesso root a recursos de aplicativos que lidam com dados confidenciais, pois um programa malicioso pode elevar privilégios no dispositivo e comprometer os recursos ou a área restrita de qualquer aplicativo. No entanto, Costa (2022) constatou que nenhum dos aplicativos do Governo Móvel possui proteção integrada para dispositivos desprotegidos (com acesso root).

A segunda recomendação é excluir quaisquer dados confidenciais armazenados e encerrar sessões do lado do servidor após alterações de estado do aplicativo. Nesse sentido, Costa (2022) observou que apenas 34% das aplicações possuem autenticação de acesso que exige que o usuário se reautentique a cada novo acesso à aplicação após fechar o aplicativo móvel.

É fundamental ressaltar que, apesar de os desenvolvedores de aplicações adotarem métodos de desenvolvimento seguros, esses, isoladamente, não garantem a proteção dos usuários. Em virtude disso, Costa (2022) menciona que é essencial analisar o comportamento de cada usuário.

Além disso, também é válido estabelecer diretrizes para os usuários de dispositivos móveis, a fim de que possam proteger sua privacidade e manter seus dispositivos seguros. Assim, o estudo de Costa (2022) recomenda as seguintes ações:

R1 - Proteger o acesso ao dispositivo
R2 - Garantir que o sistema operacional e aplicativos estejam atualizados
R3 - Evitar conectar-se a redes Wi-Fi públicas

> R4 - Instalar aplicativos de fontes confiáveis
> R5 - Evitar o rooting do dispositivo
> R6 - Desativar recursos não utilizados
> R7 - Remover aplicativos não utilizados
> R8 - Ser cuidadoso ao utilizar estações de carregamento em áreas públicas
> R9 - Avaliar atentamente as permissões de aplicativos
> R10 - Estabelecer procedimentos de emergência e descarte
> (Costa, 2022, p. 72-75)

Os resultados do estudo revelam que os aplicativos móveis do governo brasileiro precisam melhorar suas medidas de segurança para assegurar a privacidade de milhões de cidadãos. Com base nas descobertas do estudo de e nas recomendações direcionadas à Administração Pública Federal e aos usuários de aplicativos governamentais, Costa (2022) destaca a intenção de contribuir para a construção de um país que proteja a privacidade de seus cidadãos e respeite os dados pessoais.

Outro estudo sobre segurança da informação em aplicativos móveis foi conduzido por Martino (2016), que realizou uma pesquisa exploratória qualitativa selecionando esses mecanismos da base de dados da Apple, conhecida como Apple Store. Após a seleção, as políticas de privacidade de cada aplicativo foram analisadas, considerando as normas ISO/ABNT 27:002, que possuem 11 seções dedicadas ao controle de Segurança da Informação.

Martino (2016) iniciou sua pesquisa utilizando termos relacionados a aplicativos que representam bibliotecas virtuais, considerando aqueles que oferecem serviços como empréstimo, pesquisa e livros online aos usuários. Na primeira busca, com o termo “biblioteca”, foram encontrados 23 resultados, a maioria dos quais não relacionados à pesquisa.

Na segunda busca, ao utilizar o termo “biblioteca digital”, os resultados foram insatisfatórios, pois estavam todos relacionados a bibliotecas especializadas ou em línguas estrangeiras. Já na terceira e última busca, com a expressão “biblioteca virtual”, foi possível encontrar aplicativos móveis baseados em bibliotecas físicas, permitindo que os usuários explorassem suas coleções e acervos, além de aplicativos destinados à reprodução de audiolivros (Martino, 2016).

A partir dos resultados obtidos nas três etapas, Martino (2016) selecionou os três aplicativos com o maior número de downloads na Apple Store. Desse modo, o objetivo do estudo era apresentar aqueles que possuíam um grande número de usuários, assegurando, assim, que as informações fornecidas fossem confiáveis.

De acordo com Martino (2016), a próxima fase da pesquisa incluiu o estudo e avaliação das políticas de privacidade desses três aplicativos com base nas recomendações identificadas na norma ISO/ABNT 27002, com ênfase especial na segurança das informações confidenciais.

O primeiro aplicativo analisado foi a Biblioteca Virtual Universitária 3.0, que se destacou nas buscas. A seguir, a descrição que a Apple Store disponibiliza sobre o aplicativo:

> A Biblioteca Virtual disponibiliza acesso a um acervo digital com mais de 1.800 títulos em mais de 40 áreas de conhecimento, como administração, marketing, engenharia, economia, direito, letras, computação, educação, medicina, enfermagem, psicologia, psiquiatria, gastronomia, turismo e outras. Além da leitura digital dos livros, a plataforma oferece aos usuários um conjunto de funcionalidades que enriquecem a experiência de leitura. Alguns exemplos: Seleção de livros favoritos; Anotações eletrônicas nas páginas; Compartilhamento de conteúdo em redes sociais (Facebook e Twitter);· Disponibilidade de acesso 24 horas, 7 dias por semana e muito mais!. (Martino, 2016, p. 23).

Conforme destacado por Martino (2016), o aplicativo Biblioteca Virtual 3.0 tem sido amplamente baixado pelos usuários da Apple Store e, segundo os comentários, proporciona resultados satisfatórios. Na Figura 4, serão exibidos a interface do aplicativo, alguns dos livros disponíveis, além do menu e das opções de catálogo.

Figura 4 - Interface do aplicativo Biblioteca Virtual Universitária 3.0

Fonte: Martino (2016, p. 24)

O segundo aplicativo encontrado durante a pesquisa foi "Livros em Português", que, segundo Martino (2016, p. 24), conta com a seguinte descrição na Apple Store:

> [...] algumas das principais características do nosso aplicativo de armazenamento são: Filtrar por texto e livros de áudio; Seção de promoções; Pesquisa avançada; Customizável Library; Informações detalhadas sobre cada título; novos livros por semana; Operação off-line; jogue áudio em segundo plano. Pode contactar-nos por email info@libromovil.es. Todas as sugestões e comentários serão considerados para futuros lançamentos. (Martino, 2016, p. 24 e 25).

Os usuários do aplicativo expressam opiniões favoráveis, pois ele oferece ferramentas que simplificam o uso e a navegação, como os “áudio livros” e a busca especializada. Na Figura 5, são apresentados os livros mais populares e visualizados, além do menu com os livros selecionados pelo usuário.

Figura 5 - Interface do aplicativo Livros em Português

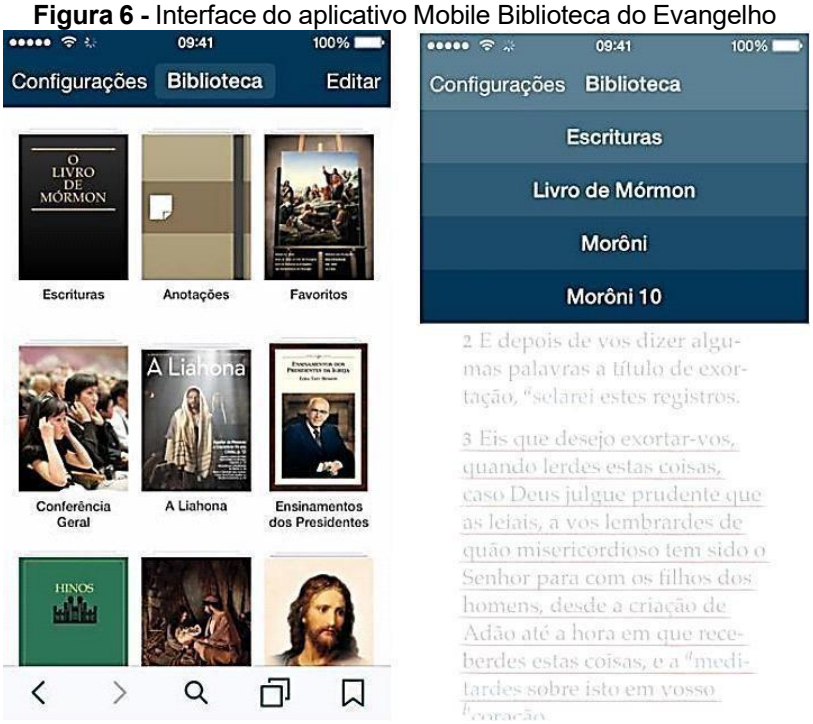
Fonte: Martino (2016, p. 25)

Por último, é possível verificar o terceiro aplicativo Mobile, denominado Biblioteca do Evangelho, Martino (2016, p. 25) verificou que a Apple Store a descreve da seguinte forma:

> [...] a Biblioteca do Evangelho é o aplicativo de estudo do evangelho de A Igreja de Jesus Cristo dos Santos dos Últimos Dias. A biblioteca inclui as escrituras, revistas da Igreja, vídeos, gravações de áudio, arte do evangelho e muito mais (Martino, 2016, p. 25).

Este aplicativo contém livros, escrituras e passagens religiosas direcionadas à Igreja de Jesus Cristo dos Santos dos Últimos Dias. Os usuários também o avaliam positivamente. Na Figura 6 abaixo, podem-se ver alguns dos livros disponíveis no terceiro aplicativo, além do menu de configurações.

Figura 6 - Interface do aplicativo Mobile Biblioteca do Evangelho



Fonte: Martino (2016, p. 26)

A Figura 6 exibe alguns dos livros disponíveis no terceiro aplicativo, bem como o menu de configurações. Adicionalmente, a Tabela 5 apresenta uma comparação fundamentada nas cinco categorias da ISO 27002.

Tabela 5 - Categorias de análise e aplicativos Mobile analisados

	Biblioteca Virtual Universitária	**Livros em Português**	**Biblioteca do Evangelho**
Política de Segurança da Informação	Não Atende	Atende	Atende
Gestão de Operações e Comunicações	Atende	Atende	Atende
Controle de Acesso	Atende	Atende	Atende
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	Não Atende	Atende	Não Atende
Gestão de Incidentes de Segurança da Informação	Atende	Atende	Atende

Fonte: Martino (2016, p. 28)

Martino (2016) evidenciou a análise baseada nas Políticas de Privacidade dos três aplicativos mencionados. Na Apple Store, há apenas uma seção de Política de Privacidade para o aplicativo Biblioteca Universitária Virtual 3.0; contudo, ao clicar no link fornecido, encontra-se a mesma versão da “descrição” do aplicativo, conforme exibida na página inicial da Apple Store.

Essa situação demonstra negligência com o consumidor e com a proteção da privacidade dos dados do usuário, especialmente por ser um dos aplicativos mais baixados na Apple Store, mas que não possui uma política de privacidade ou, pelo menos, não a divulga. Com isso, na ausência de uma Política de Privacidade, quaisquer incidentes envolvendo o uso das informações do usuário tendem a se agravar.

Sobre o segundo aplicativo analisado, Martino (2016) aponta que, apesar de o aplicativo Livros em Português estar inteiramente em português, sua política de privacidade está escrita em inglês. Essa atitude demonstra uma clara indiferença em relação aos brasileiros. Embora o inglês seja uma língua amplamente falada, muitos usuários desse aplicativo não dominam o idioma, tornando a política de privacidade difícil de entender e inadequada.

Por outro lado, no aplicativo Biblioteca do Evangelho, os usuários encontram uma Política de Privacidade completa e detalhada, organizada em seções, o que facilita a compreensão. Além de receber avaliações positivas na Apple Store, o aplicativo esclarece aos usuários quais dados são protegidos e de que forma (Martino, 2016).

Conforme o estudo de Martino (2016) sobre aplicativos de biblioteca, observa-se que, apesar das vulnerabilidades na segurança de acesso e no *download* por redes desconhecidas, a maioria dos aplicativos cumpre as categorias de proteção estabelecidas na Tabela 5.

Entretanto, é importante destacar que todas as informações do usuário ficam vulneráveis quando o dispositivo móvel é entregue a terceiros. Portanto, a segurança da informação deve ser priorizada em relação aos diferentes tipos de permissões de acesso disponíveis.

Martino (2016) também enfatiza que um ambiente de biblioteca altamente seguro deve cumprir todas as disposições da ISO 27002:2013 aplicáveis aos

sistemas de bibliotecas. Dessa forma, os usuários podem baixar aplicativos móveis em seus dispositivos com maior segurança.

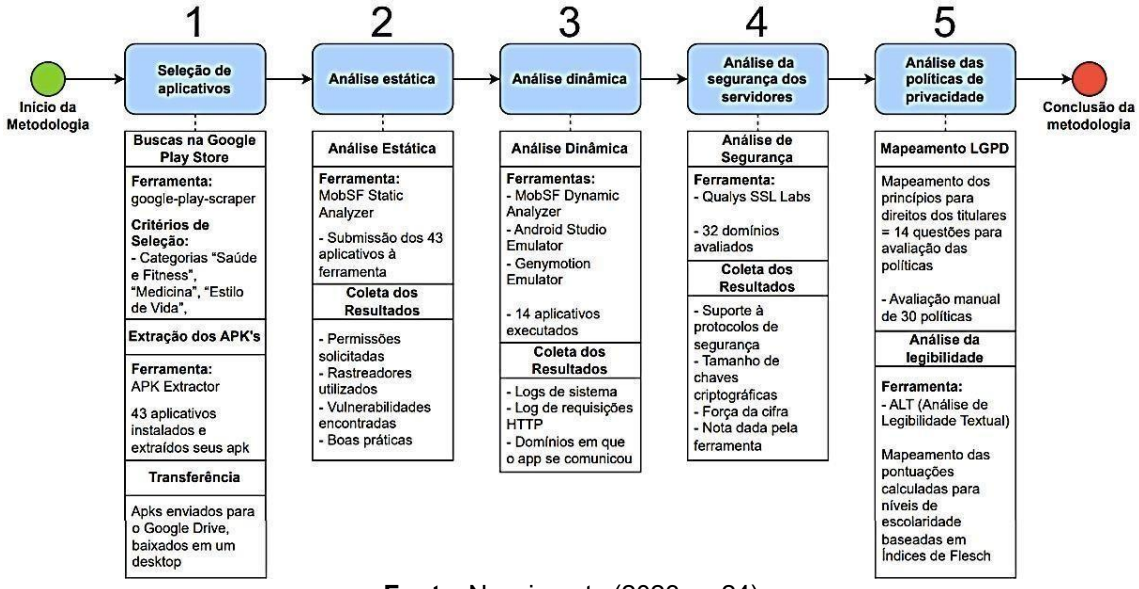
Em relação aos estudos sobre a segurança em aplicativos móveis, Nascimento (2023) destaca que eles são voltados para a saúde mental (mHealth apps) estão se tornando ferramentas essenciais para melhorar o bem-estar das pessoas em um mundo cada vez mais tecnológico e dependente de dispositivos móveis. Durante a pandemia de COVID-19, esses aplicativos cresceram significativamente, oferecendo desde exames de saúde física até apoio emocional.

Apesar de sua relevância, há preocupações quanto à privacidade dos usuários e à segurança dos dados com o rápido crescimento dos aplicativos de saúde mental. É crucial verificar se os rastreadores e perfis cumprem as leis de privacidade, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil.

O estudo de Nascimento (2023) teve como objetivo identificar as vulnerabilidades de segurança e privacidade nos aplicativos de saúde mental mais baixados no Brasil, disponíveis na Google Play Store para dispositivos Android, avaliando a conformidade com os princípios da LGPD e os direitos dos titulares dos dados pessoais.

Na Figura 7, Nascimento (2023) apresenta a metodologia utilizada na pesquisa, dividida em cinco etapas:

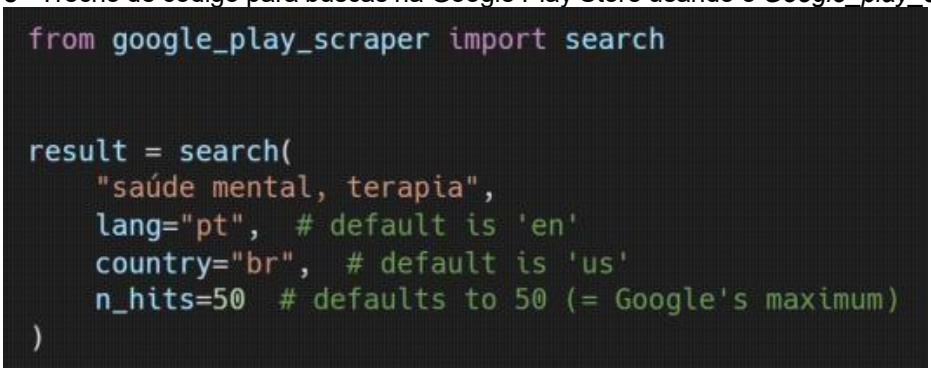
Figura 7 - Etapas da metodologia adotada para analisar os aplicativos Mobile de saúde mental



Fonte: Nascimento (2023, p. 24)

O passo inicial consistiu em escolher a ferramenta em questão voltada à saúde mental disponíveis na Google Play Store do Brasil. Para realizar essa seleção, utilizou-se a biblioteca google_play_scraper juntamente com o Python 3.10. Essa ferramenta limita a busca a 50 aplicativos, conforme a restrição imposta pelo Google Play. A Figura 8 ilustra o código utilizado para pesquisar por “saúde mental” e “terapia” em português do Brasil.

Figura 8 - Trecho de código para buscas na Google Play Store usando o *Google_play_scraper*



```
from google_play_scraper import search


result = search(
    "saúde mental, terapia",
    lang="pt",  # default is 'en'
    country="br",  # default is 'us'
    n_hits=50  # defaults to 50 (= Google's maximum)
)
```

Fonte: Nascimento (2023, p. 25)

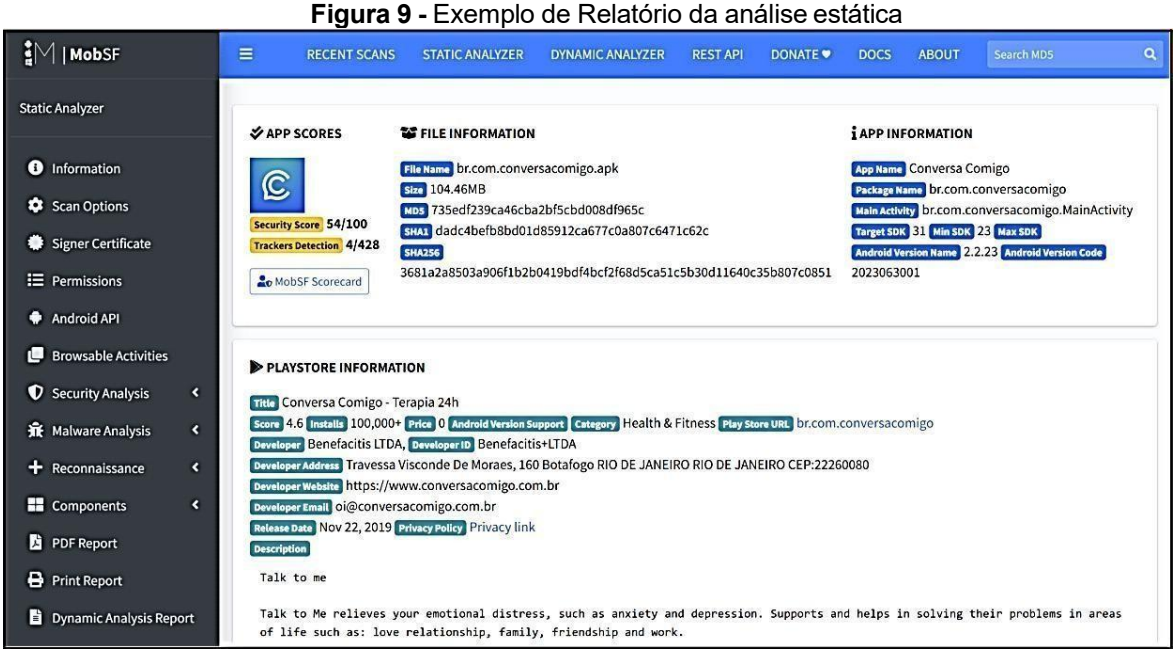
Conforme Nascimento (2023), os selecionados deveriam ser gratuitos e pertencer às categorias de saúde e fitness, medicina, estilo de vida, ferramentas e educação. Testes de QI, testes de conhecimento e aplicativos fora do tema mHealth foram excluídos. Dos 50 aplicativos de saúde mental retornados, 43 foram escolhidos para análise.

Nas etapas seguintes, foi necessário instalar os 43 aplicativos e extrair seus pacotes APK. Utilizou-se um smartphone Samsung Galaxy S10 Lite, com configurações de fábrica e uma conta Google fornecida pela universidade do aluno. Com o extrator APK, todos os 43 arquivos foram extraídos e salvos no Google Drive. Para o *download* dos arquivos, foram usados um processador Ryzen 7 5800X e Windows 10 Professional (Nascimento, 2023).

Nascimento (2023) ressalta que, para a análise estática e dinâmica da segurança dos aplicativos Android e iOS, foi utilizado o MobSF (Mobile Security Framework), uma ferramenta de código aberto amplamente usada na academia e na indústria. O MobSF detecta vulnerabilidades conhecidas e padrões de código suspeitos, oferecendo recursos avançados de análise. A ferramenta verifica automaticamente o código-fonte, comparando-o com um banco de dados extenso de ameaças conhecidas.

Na análise estática, os 43 arquivos APK foram submetidos à interface web do MobSF, que processou e exibiu os resultados rapidamente. A Figura 9 mostra um dashboard com os resultados da análise, incluindo comentários sobre a qualidade do código, métodos de programação, regulamentos de segurança e conformidade com as melhores práticas.

Figura 9 - Exemplo de Relatório da análise estática



Fonte: Nascimento (2023, p. 26)

Para realizar a análise dinâmica, foi necessário configurar um emulador Android. Duas ferramentas de emulação compatíveis com o MobSF foram testadas: Genymotion Android e Android Studio Emulator. Observou-se que o Genymotion é fácil de instalar, mas suporta apenas aplicativos Android x86 e x86_64.

Em contrapartida, o Android Studio oferece suporte às arquiteturas arm, arm64, x86 e x86_64, permitindo a análise de um maior número de aplicações. Por essa razão, apesar de ser um pouco mais complexo, o Android Studio foi escolhido.

Nascimento (2023) menciona que, durante a simulação, utilizou-se um Samsung Galaxy S10, rodando Android API29 (versão 10.0), como dispositivo de emulação. O MobSF fornece uma interface para selecionar um aplicativo, instalá-lo em um emulador Android e executá-lo.

Durante a análise dinâmica, alguns aplicativos apresentaram problemas, como telas brancas e falhas ao tentar utilizá-los. Segundo Nascimento (2023), esses problemas podem ocorrer devido a medidas de segurança implementadas nos

aplicativos, como scripts ao usar um emulador, acesso root ativado ou a ausência dos Google Play Services no dispositivo. Como resultado, apenas 14 dos 43 aplicativos móveis foram executados com sucesso.

Todos os 14 aplicativos testados passaram por uma avaliação completa, onde todos os recursos gratuitos foram utilizados, todas as telas foram navegadas e todos os botões foram clicados. A Figura 10 mostra a interface onde o usuário pode acessar o log e o histórico das solicitações HTTP feitas pela aplicação durante a interação.

Figura 10 - Exemplo de Relatório da análise dinâmica

Fonte: Nascimento (2023, p. 26)

Entre os 43 aplicativos selecionados, foram incluídos aqueles voltados para meditação, monitoramento de humor, diários de saúde, gerenciamento de ansiedade e diversos outros relacionados à saúde mental. Nascimento (2023) decidiu não divulgar certas informações sobre os aplicativos para proteger a privacidade dos usuários e evitar possíveis danos.

Com base nas instalações e análises, o Quadro 1 apresenta um resumo dos principais recursos desses mecanismos, incluindo *downloads*, classificações e avaliações de usuários. As páginas da Google Play Store oferecem descrições, *downloads*, comentários de usuários, capturas de tela e outras informações sobre os aplicativos, além do número de *downloads* fornecido pelo desenvolvedor.

Quadro 1 - Relação de aplicativos selecionados

APP_ID	Gênero	Quantidade de Instalações	Avaliação pelos usuários	Quantidade de Avaliações
APP_1	Saúde e fitness	10.000.000+	4.8	539.000+
APP_2	Saúde e fitness	5.000.000+	4.8	182.000+
APP_3	Estilo de vida	5.000.000+	4.6	153.000+
APP_4	Saúde e fitness	1.000.000+	4.9	227.000+
APP_5	Saúde e fitness	1.000.000+	4.8	144.000+
APP_6	Medicina	1.000.000+	4.9	57.100+
APP_7	Saúde e fitness	1.000.000+	4.4	48.700+
APP_8	Saúde e fitness	1.000.000+	4.1	38.400+
APP_9	Saúde e fitness	1.000.000+	4.5	32.400+
APP_10	Saúde e fitness	1.000.000+	4.3	29.000+
APP_11	Estilo de vida	1.000.000+	4.3	25.700+
APP_12	Saúde e fitness	1.000.000+	3.9	16.100+
APP_13	Saúde e fitness	1.000.000+	4.2	8.930
APP_14	Educação	1.000.000+	3.3	5.710
APP_15	Saúde e fitness	500.000+	3.2	10200+
APP_16	Estilo de vida	500.000+	4.8	9.480
APP_17	Saúde e fitness	500.000+	4.1	6.890
APP_18	Saúde e fitness	500.000+	4.4	3.290
APP_19	Saúde e fitness	100.000+	4.3	7.250
APP_20	Medicina	100.000+	4.1	5.200
APP_21	Saúde e fitness	100.000+	4.5	5.070
APP_22	Saúde e fitness	100.000+	4.7	3.320
APP_23	Saúde e fitness	100.000+	4.4	3.180
APP_24	Saúde e fitness	100.000+	3.7	2.320
APP_25	Medicina	100.000+	4.8	1.890
APP_26	Saúde e fitness	100.000+	4.9	1.830
APP_27	Estilo de vida	100.000+	4.7	1.390
APP_28	Medicina	100.000+	4.5	1.263
APP_29	Saúde e fitness	100.000+	3.1	472
APP_30	Saúde e fitness	50.000+	3.5	292
APP_31	Educação	50.000+	4.5	266
APP_32	Saúde e fitness	50.000+	4.5	127
APP_33	Estilo de vida	10.000+	4.7	379.000+
APP_34	Estilo de vida	10.000+	4.3	2.260
APP_35	Saúde e fitness	10.000+	3.0	582
APP_36	Estilo de vida	10.000+	3.0	120
APP_37	Saúde e fitness	10.000+	3.4	99
APP_38	Saúde e fitness	10.000+	0	0
APP_39	Saúde e fitness	10.000+	0	0
APP_40	Ferramentas	1.000+	4.7	29
APP_41	Saúde e fitness	1.000+	4.8	10
APP_42	Saúde e fitness	1.000+	0	0
APP_43	Saúde e fitness	1.000+	0	0

Fonte: Nascimento (2023, p. 37)

De acordo com Nascimento (2023), os aplicativos móveis voltados para a saúde mental são categorizados em 36 “etiquetas” que definem o alcance de cada

programa. O Quadro 2 apresenta um resumo dos resultados obtidos por esse método, sem a necessidade de novas etiquetas.

Quadro 2 - Etiquetas usadas na análise dos 43 aplicativos

Etiquetas	Frequência de Apps	Iwaya et al. (2022)
Rastreador de humor e hábito	49%	44%
Ansiedade	49%	81%
Estresse e *Burnout*	37%	70%
Terapia online	30%	30%
Depressão	28%	48%
Meditação	25,5%	30%
Diário, agenda e planejamento pessoal	25,5%	48%
Distúrbios, vício, bipolaridade, raiva, fobia, distúrbios alimentares, emoções negativas, transtorno de humor, automutilação, TEPT, TOC e TDAH	25,5%	37%
Avaliação de saúde mental, diagnóstico e verificação de sintomas	23,25%	11%
Chatbot	21%	19%
Distúrbios de Sono e Insônia	16,3%	48%
Autoestima e ânimo	16,3%	15%
Ataques de pânico	4,65%	30%

Fonte: Nascimento (2023, p. 39)

Conforme Nascimento (2023), dos 43 aplicativos móveis avaliados, 21 (49%) tratam da ansiedade e permitem aos usuários monitorar o humor e hábitos. Uma parcela significativa de 16 (37%) está voltada para o estresse e burnout.

Além disso, alguns aplicativos oferecem terapia online com psicólogos, meditação, diários, planos pessoais e utilizam "*chatbots"* para diagnosticar diversas doenças, além de ajudar na autoestima e no gerenciamento de ataques de pânico.

Durante a análise estática, Nascimento (2023) examinou as permissões solicitadas pelos aplicativos, identificando rastreadores utilizados, vulnerabilidades de código e boas práticas de codificação. Vale destacar que, na análise das Políticas de Privacidade, foi constatado que dos 13 desenvolvedores dos 43 aplicativos móveis, nenhum forneceu uma política de privacidade. Desse modo, a análise foi realizada apenas nas 30 políticas disponíveis.

Segundo Nascimento (2023), a análise das políticas de privacidade foi totalmente manual e o texto era pesquisável. Além disso, a análise dinâmica da solicitação foi realizada enquanto a solicitação ainda estava em execução, indicando que as vulnerabilidades e comportamentos identificados refletiram apenas o estado da aplicação no momento do uso. Assim, o comportamento do aplicativo após longos períodos de inatividade não foi testado, o que pode revelar possíveis vulnerabilidades latentes.

Os três estudos realizados permitiram constatar que a análise dos aplicativos móveis demonstra que, independentemente da área de atuação de cada um, existem limitações e desafios na segurança, especialmente no que se refere à Política de Privacidade e Segurança da Informação.

CONCLUSÃO

O estudo buscou responder à seguinte questão: Os usuários de aplicativos móveis e da internet estão sendo protegidos pelas Políticas de Privacidade dos aplicativos disponíveis para *download* e pela Segurança da Informação?

Com base na análise do desenvolvimento e uso atual dos aplicativos móveis, bem como na compreensão dos padrões de Segurança da Informação e sua aplicação nas Políticas de Privacidade, ficou claro que há uma necessidade contínua de aprimorar essas políticas e sua eficácia. Isso foi especialmente evidenciado pelos estudos sobre a segurança e privacidade dos dados dos usuários em certos aplicativos.

Por exemplo, a pesquisa que examinou os aplicativos do Governo Móvel revelou que, apesar de serem criados por órgãos governamentais, há falhas significativas na privacidade e na Segurança da Informação, expondo os usuários a possíveis ataques de hackers e outras ameaças cibernéticas.

Nessa perspectiva, a proteção dos aplicativos móveis não é responsabilidade exclusiva dos engenheiros e desenvolvedores; ela também depende da conscientização e do comportamento dos usuários. Além disso, o uso negligente pode expor dados pessoais, facilitando, assim, o acesso indevido por terceiros mal-intencionados.

Em virtude disso, é crucial que os usuários possuam alfabetização digital para identificar ameaças e fraudes, diminuindo assim os riscos de invasão aos aplicativos que utilizam. Simultaneamente, os desenvolvedores e as empresas responsáveis devem revisar e atualizar continuamente suas Políticas de Privacidade, além de adotar técnicas de segurança mais avançadas para proteger os usuários.

Portanto, a responsabilidade pela segurança da informação é compartilhada entre desenvolvedores e usuários. Desse modo, ambos devem estar cientes dos riscos e agir proativamente para garantir a proteção dos dados trocados por meio de aplicativos móveis. Caso essa proteção não seja assegurada, as consequências podem ser graves tanto para os usuários quanto para as empresas envolvidas.

REFERÊNCIAS

BEAL, A. **Segurança da Informação:** princípios e melhores práticas, 2005.

CAVALCANTE, Alexandre Ferreira. **Guia de Segurança da Informação em Dispositivos Móveis Dentro Das Corporações.** 2019. 63f. Monografia (Bacharelado em Ciência da Computação) - Programa de Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco, Recife, 2019. Disponível em: https://www.cin.ufpe.br/~tg/2019-1/TG_CC/tg_afc2.pdf. Acesso em: 04 jul. 2024.

COSTA, Carlos Humberto Lopes. **Análise de segurança e privacidade de aplicativos móveis do governo brasileiro.** 2022. 86f. Dissertação (Mestrado em Informática) - Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná, Curitiba-PR, 2022. Disponível em: https://acervodigital.ufpr.br/handle/1884/80921. Acesso em: 08 jul. 2024.

CUNHA, Suellen Maria Dominguez. **Desenvolvimento de aplicativo mobile para controlar o uso das redes sociais.** TCC de Graduação (Design) - Universidade Federal do Amazonas, Manaus, 2022. Disponível em: https://www.riu.ufam.edu.br/bitstream/prefix/6363/7/TCC_Suellen%20Maria%20Dominguez%20Cunha.pdf. Acesso em: 04 jul. 2024.

FLING, Brian. **Mobile design and development:** practical techniques of creating mobile sites and web apps. p. 37-39, 2009.

GRACIANO, Renan Felipe Coglioni. **Aplicação de técnicas de segurança no desenvolvimento de um aplicativo Android.** 2017. 58f. Monografia (Curso de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza, Americana, SP, 2017. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/771/1/20171S_GRACIANORenanFelipeCoglioni_OD0205.pdf. Acesso em: 04 jul. 2024.

KESANIEMI, A.; MÁKELÁ, J. **Mobile Application Threat Analysis.** OWASP Helsinki Chapter Meeting. 2011. Disponível em: https://owasp.org/www-pdf-archive/Mobilethreat-analysis-short-presentation_owasp.pdf. Acesso em: 04 jul. 2024.

LEAVITT, Neal. Mobile security: finally a serious problem? **IEEE Computer Society**, v. 44, p. 11-14, 2011. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5875929. Acesso em: 08 jul. 2024.

LIPNER, S.; HOWARD, M. **O ciclo de vida do desenvolvimento da segurança de computação confiável.** 2005. Disponível em: https://msdn.microsoft.com/pt-br/library/ms995349.aspx. Acesso em: 08 jul. 2024.

MARTINO, Clarissa Lins Cardozo. **Segurança da informação em aplicativos de dispositivos móveis.** Trabalho de Conclusão de Curso (Graduação em Biblioteconomia) – Curso de Biblioteconomia e Gestão de Unidades de Informação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, 2016. Disponível em:

https://pantheon.ufrj.br/bitstream/11422/182/1/nova%20vers%c3%a3o%20TCC%20Clarissa%202016%20final%20revisada.pdf. Acesso em: 04 jul. 2024.

MATOS NETO, Eurico. **Governo móvel no Brasil:** uma análise do estado da arte no desenvolvimento de aplicativos móveis por instituições do setor público brasileiro. Tese de doutorado, Universidade Federal da Bahia. 2020. Disponível em: https://repositorio.ufba.br/handle/ri/34960. Acesso em: 08 jul. 2024.

MINAYO, M. C. DE S. Análise qualitativa: teoria, passos e fidedignidade. **Ciência & Saúde Coletiva**, v. 17, n. 3, p. 621–626, mar. 2012. Disponível em: https://www.scielo.br/j/csc/a/39YW8sMQhNzG5NmpGBtNMFf/#ModalHowcite. Acesso em: 08 jul. 2024.

MORIMOTO C. E. **Smartphones, Guia Prático.** Porto Alegre: GDH Press e Sul Editores, p. 432, 2009.

NASCIMENTO, Gustavo Prazeres Paz do. **Uma investigação empírica sobre. privacidade em aplicativos de saúde mental no Brasil.** 2023. 72f. Monografia (Graduação em Sistemas de Informação) - Universidade Federal de Pernambuco, Centro de Informática, Recife, 2023. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/52753/9/TCC%20Gustavo%20Prazeres%20Paz%20do%20Nascimento.pdf. Acesso em: 08 jul. 2024.

TARANDACH, I.; COLES, M. **Threat Modeling:** A Practical Guide for Development Teams. O'Reilly Media, Incorporated. 2020.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Monteiro - Código INEP: 25284940
Pb-264, S/N, Serrote, CEP 58500-000, Monteiro (PB)
CNPJ: 10.783.898/0008-41 - Telefone: (83) 3351-3700

Documento Digitalizado Ostensivo (Público)

Trabalho de conclusão de curso

Assunto:	Trabalho de conclusão de curso
Assinado por:	Francisco Chaves
Tipo do Documento:	Dissertação
Situação:	Finalizado
Nível de Acesso:	Ostensivo (Público)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Francisco Lucas da Silva Chaves, ALUNO (202015020009) DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS - MONTEIRO**, em 02/04/2025 19:47:30.

Este documento foi armazenado no SUAP em 02/04/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1445750
Código de Autenticação: 6e4d69ec47