Modelagem de ameaças à privacidade e à segurança em aplicativos móveis: uma abordagem orientada à LGPD

Lucas de Castro Carvalho[1], **Josiane da Costa Vieira Rezende**[1], **Air Rabelo**[1]

[1] Programa de Pós-Graduação Stricto Sensu em
Tecnologia da Informação e Comunicação e Gestão do Conhecimento
Universidade FUMEC
Belo Horizonte – MG – Brasil

empresarial.lucascarvalho@gmail.com, josianecvieira@gmail.com

air@fumec.br

Abstract. *Mobile applications process personal data in environments marked by continuous connectivity, device capabilities, local storage, and third-party services. Anticipating security and privacy threats during development remains a relevant challenge. This article proposes a complementary LGPD-oriented approach to threat modeling in mobile applications. The approach is organized into four analytical movements that connect scope, assets, personal data flows, security and privacy threats, technical controls, and LGPD requirements. Grounded in a narrative literature review and documentary research, the proposal was conceptually assessed through the Mais Saúde scenario. The assessment examined coverage of the four movements, traceability, joint treatment of security and privacy, mobile-specific characteristics, operationalization, and internal coherence. The results indicate that the approach can organize outputs from established methods into a technical-normative traceability chain. Its scope, however, remains limited to a conceptual assessment.*

Resumo. *Aplicativos móveis processam dados pessoais em ambientes marcados por conectividade contínua, recursos do dispositivo, armazenamento local e serviços de terceiros. Antecipar ameaças à segurança e à privacidade durante o desenvolvimento permanece um desafio relevante. Este artigo propõe uma abordagem complementar orientada à LGPD para a modelagem de ameaças em aplicativos móveis. A proposta está organizada em quatro movimentos analíticos que relacionam escopo, ativos, fluxos de dados pessoais, ameaças de segurança e privacidade, controles técnicos e exigências da LGPD. Fundamentada em revisão bibliográfica narrativa e pesquisa documental, a abordagem foi avaliada conceitualmente no cenário Mais Saúde. A avaliação examinou a cobertura dos quatro movimentos, a rastreabilidade, o tratamento conjunto de segurança e privacidade, as particularidades do ambiente móvel, a operacionalização e a coerência interna. Os resultados indicam que a proposta pode organizar resultados de métodos consolidados em uma cadeia de rastreabilidade técnico-normativa. Seu alcance, contudo, permanece restrito a uma avaliação conceitual.*

1. Introdução

Aplicativos móveis combinam coleta de dados, autenticação, armazenamento local, comunicação com serviços remotos e integração com componentes externos, ampliando os pontos de tratamento e exposição de dados pessoais. Cerqueira, Mello e Travassos registram que há "pouco ou nenhum suporte para isto na prática" [Cerqueira et al. 2023]. Essa lacuna dificulta a aproximação entre exigências da LGPD e decisões técnicas.

A modelagem de ameaças oferece meios para antecipar esses problemas. Métodos consolidados, como STRIDE, LINDDUN e PASTA, são considerados neste trabalho como referências complementares. A lacuna investigada não está na ausência de métodos, mas na necessidade de relacionar seus resultados às particularidades do ambiente móvel e às exigências da LGPD. Rodrigues, Villela e Feitosa observam que técnicas generalistas "não possuem características específicas para tratar ameaças de privacidade em nível de design" [Rodrigues et al. 2023].

Diante disso, o artigo propõe uma abordagem complementar que organiza a relação entre ativos, fluxos de dados pessoais, ameaças, controles técnicos e exigências da LGPD em aplicativos móveis. O objetivo é estabelecer uma cadeia de rastreabilidade entre ponto de exposição, ameaça identificada, resposta técnica e fundamento normativo, sem substituir os métodos existentes. A proposta foi formulada por meio de pesquisa bibliográfica e documental e submetida a uma avaliação conceitual em um cenário da área da saúde.

2. Fundamentação teórica

2.1. Aplicativos móveis, dados pessoais e exigências da LGPD

A expansão dos aplicativos móveis ampliou a coleta, a circulação e o compartilhamento de dados pessoais entre dispositivo, aplicativo e serviços externos. No Brasil, esse cenário passou a ser diretamente tensionado pela Lei Geral de Proteção de Dados Pessoais. Sá afirma que a LGPD "traz novas regras sobre a coleta e o tratamento de dados pessoais por empresas e por órgãos públicos" [de Sá 2019]. No contexto móvel, isso repercute em decisões relacionadas à coleta, ao uso, ao armazenamento, à transmissão e ao descarte ao longo do funcionamento do sistema.

Interface, sensores, armazenamento local, APIs, componentes de terceiros e serviços em nuvem compõem percursos informacionais nem sempre visíveis para o usuário. Moura e Coutinho observam que a proteção de dados constitui "um aspecto a ser considerado dentro do processo de desenvolvimento de aplicações e sistemas" e afirmam que incorporar elementos da lei desde o início do processo é "algo essencial" [de Moura and Coutinho 2024]. Cerqueira, Mello e Travassos acrescentam que a evolução do tema exige "novas tecnologias para garantir a qualidade do software" [Cerqueira et al. 2023]. Não basta, portanto, reconhecer a incidência da LGPD sobre aplicativos móveis; é necessário aproximar suas exigências das práticas de desenvolvimento.

A relação entre base legal, finalidade e transparência amplia o problema. Teffé e Viola ressaltam que a LGPD funciona como "instrumento de controle sobre as suas informações pessoais e de garantia de direitos" [Teffé and Viola 2020]. Oliveira, Ferreira e Pires afirmam que "é necessária uma relação lógica entre o tratamento dos dados, as

finalidades objetivas e a informação dada ao titular" [Oliveira et al. 2021]. O problema, portanto, não se resume à existência de conteúdo pessoal no sistema, mas alcança as condições sob as quais ele é utilizado, mantido e justificado perante o titular.

A transparência percebida pelo usuário também é afetada por essa dificuldade. Jardim et al., ao analisarem políticas de privacidade de aplicativos utilizados no Brasil, identificaram que "nenhuma política foi classificada como sendo de fácil leitura" [Jardim et al. 2022]. No mesmo estudo, os autores mostram que os problemas encontrados "desestimulam a leitura" e "dificultam a compreensão das práticas de dados" [Jardim et al. 2022]. No plano prático, o Guia de Boas Práticas da LGPD no Setor Público estabelece a necessidade de "identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais" [Brasil 2018]. Esse direcionamento reforça a importância de aproximar operações concretas, avaliação de risco e proteção do titular.

2.2. Modelagem de ameaças à segurança e à privacidade como resposta técnica

A modelagem de ameaças ganha relevância quando a leitura de riscos precisa ocorrer antes da consolidação da solução. Alves et al. definem *Threat Modeling* como "uma prática estruturada de identificar e avaliar possíveis ameaças à segurança de um sistema" [Alves et al. 2024]. No mesmo trabalho, afirmam que essa prática busca "determinar as medidas necessárias para mitigar essas ameaças" [Alves et al. 2024]. Seu valor, nesse sentido, está em apoiar a passagem entre reconhecimento do problema e definição de medidas de proteção.

A distância entre texto normativo e implementação torna essa utilidade mais nítida. Cerqueira, Mello e Travassos apontam uma "lacuna persistente nas práticas de implementação dos direitos, deveres e responsabilidades previstos na LGPD em sistemas de software" e destacam a "falta de metodologias que suportem a implementação destes conceitos nos diferentes estágios do ciclo de vida de software" [Cerqueira et al. 2023]. Nesse contexto, a modelagem de ameaças funciona como meio de aproximar exigência regulatória, decisão de projeto e elemento técnico do sistema.

A entrada da privacidade nessa leitura traz contornos mais específicos. Rodrigues, Villela e Feitosa observam que propostas generalistas "não possuem características específicas para tratar ameaças de privacidade em nível de design" e afirmam que "uma técnica amplamente usada nesse contexto é a modelagem de ameaças" [Rodrigues et al. 2023]. No mesmo estudo, os autores definem ameaça à privacidade como "um evento indesejável potencial ou real" capaz de gerar "divulgação, exposição e uso indevido de dados privados do usuário" [Rodrigues et al. 2023]. Isso ajuda a mostrar que, embora segurança e privacidade se cruzem, a segunda exige atenção mais direta à coleta excessiva, ao compartilhamento inadequado, ao reuso indevido, à inferência e à opacidade no uso das informações.

A literatura também indica que a modelagem de ameaças deve integrar o processo de desenvolvimento. Alves et al. afirmam que essa prática "deve ser integrada em várias fases do desenvolvimento de software" [Alves et al. 2024]. Santos, Prado e Chaim observam que "aplicações seguras são resultado da decisão de produzi-las por parte da organização" [Santos et al. 2020]. De França e Da Silva acrescentam que "a construção da imagem da aplicação só ocorrerá se os jobs de segurança forem realizados com sucesso" [De França and Da Silva 2022]. Em conjunto, esses resultados indicam que medi-

das de proteção devem compor o fluxo regular de desenvolvimento e entrega.

Cerqueira, Mello e Travassos destacam que a Privacidade desde a Concepção busca orientar sua implementação "desde os primeiros passos da construção de um produto" e propõe "elevar a privacidade a um objetivo principal" [Cerqueira et al. 2023]. O estudo também ressalta a necessidade de uma "tradução efetiva de princípios abstratos de privacidade" em "requisitos implementáveis" [Cerqueira et al. 2023]. Moura e Coutinho acrescentam que "o conhecimento em LGPD é necessário para que RF e RNF estejam alinhados a seus princípios" e que "os modelos, textos e diagramas gerados nesse momento devem refletir aspectos da LGPD dentro do sistema" [de Moura and Coutinho 2024].

Neste artigo, esses elementos fundamentam a relação com a Privacidade desde a Concepção (*Privacy by Design*) e a Privacidade por Padrão (*Privacy by Default*), tratadas como referências para antecipar decisões de proteção, limitar o tratamento e registrar sua justificativa.

A ENISA situa a Engenharia de Proteção de Dados no âmbito da proteção desde a concepção e por padrão e afirma que ela "aims to support the selection, deployment and configuration of appropriate technical and organizational measures" [European Union Agency for Cybersecurity (ENISA) 2022]. Embora o relatório tenha o GDPR como referência jurídica, neste artigo seus princípios técnicos são reancorados na LGPD. Essa leitura reforça a passagem entre princípios de proteção de dados, requisitos implementáveis e controles técnicos, sem deslocar o eixo normativo brasileiro.

2.3. Posicionamento em relação a métodos consolidados de modelagem de ameaças

A proposta não busca substituir métodos consolidados de modelagem de ameaças. Seu papel é complementar: organizar a relação entre resultados produzidos por essas abordagens, particularidades do ambiente móvel, respostas técnicas e exigências da LGPD.

A Microsoft afirma que o STRIDE "categorizes different types of threats and simplifies the overall security conversations" [Microsoft 2023]. O trabalho original do LINDDUN declara que a abordagem "provides a systematic methodology to model privacy-specific threats" [Deng et al. 2011]. O próprio subtítulo do PASTA o define como "Process for Attack Simulation and Threat Analysis" [UcedaVelez and Morana 2015]. Assim, STRIDE apoia a classificação de ameaças de segurança, LINDDUN direciona a análise de privacidade e PASTA acrescenta uma perspectiva orientada a ataques e riscos.

Para fins de comparação, os movimentos da proposta são representados por M1, delimitação da análise; M2, identificação de ativos, dados pessoais e fluxos; M3, identificação de ameaças; e M4, correlação entre ameaças, controles e exigências da LGPD. A Tabela 1 sintetiza a relação entre os métodos e a estrutura proposta.

STRIDE, LINDDUN e PASTA fornecem mecanismos próprios para identificar, detalhar ou priorizar ameaças. A proposta não reproduz esses mecanismos; organiza seus possíveis resultados em uma cadeia de rastreabilidade entre ameaça, decisão de proteção e fundamento normativo associado ao tratamento de dados pessoais em aplicativos móveis.

2.4. Particularidades do ambiente móvel

Aplicativos móveis não podem ser tratados como simples extensão de sistemas tradicionais, porque operam em um cenário com restrições e superfícies de exposição próprias.

Tabela 1. Posicionamento da proposta em relação a métodos consolidados

Abordagem	Foco e entrada	Resultado principal	Relação com a proposta
STRIDE	Segurança do desenho; componentes, fluxos e limites de confiança.	Ameaças de segurança classificadas e possíveis mitigações.	Apoia M1 e M2 na representação do sistema e M3 na identificação de ameaças de segurança. Suas mitigações podem alimentar M4.
LINDDUN	Privacidade; fluxos de dados e interações entre elementos.	Ameaças de privacidade e possíveis contramedidas.	Apoia M2 no exame dos fluxos, M3 na identificação de ameaças à privacidade e M4 na definição de respostas de proteção.
PASTA	Risco; objetivos de negócio, escopo, arquitetura, ameaças e vulnerabilidades.	Cenários de ataque, análise de impacto e contramedidas priorizadas.	Apoia M1 na delimitação, M2 na decomposição, M3 na análise de ameaças e M4 na priorização das respostas.
Proposta	Ambiente móvel, dados pessoais, ameaças, controles e LGPD.	Cadeia de rastreabilidade entre exposição, ameaça, resposta técnica e exigência normativa.	Utiliza resultados dos métodos anteriores e acrescenta a associação explícita com particularidades do ambiente móvel e exigências da LGPD.

Dispositivos pessoais, conectividade contínua, sensores, permissões e dependência de serviços externos compõem um quadro em que problemas ligados à proteção do conteúdo exigem leitura específica.

Limitações técnicas interferem diretamente no desenho da solução. Andrade, Agra e Malheiros observam que dispositivos móveis apresentam "limitações de memória, bateria, processamento, tamanho de tela e teclado, capacidade de armazenamento [...] e consumo de energia" [Andrade et al. 2013]. Esses fatores influenciam decisões sobre processamento local ou remoto, frequência de sincronização, uso de armazenamento persistente e escolha de mecanismos de proteção compatíveis com a capacidade do dispositivo. Permissões, sensores e funcionalidades do sistema operacional também atravessam o uso da informação nesse cenário. Silva, Rosa, Ferneda e Braga Filho registram que "71% dos aplicativos avaliados manipulam e compartilham dados pessoais de seus usuários, mesmo sem ter políticas de privacidade" [Silva et al. 2018], o que reforça que permissões e integrações ampliam o alcance da exposição para além do ponto inicial de coleta.

Problemas recorrentes já foram registrados pela literatura de segurança nesse campo. Ferreira, Santos e Choren afirmam que o OWASP Mobile Top Ten "tem por objetivo auxiliar desenvolvedores a entender os riscos mais críticos que aplicativos móveis podem apresentar" [Ferreira et al. 2017]. Isso reforça que o ambiente móvel não deve ser tratado como mera variação de sistemas web ou desktop, pois reúne vulnerabilidades recorrentes e vetores próprios de exploração, como armazenamento inseguro, comunicação inadequadamente protegida, autenticação fraca, exposição excessiva de dados e uso indevido de permissões. Em chave complementar, Marques e Santana afir-

mam que "os dispositivos móveis tornam-se altamente visados por criminosos digitais" [Marques and Santana 2023], observação que ajuda a ligar características do domínio a possibilidades concretas de interceptação e exploração.

O desenvolvimento seguro, nesse cenário, deixa de ser preocupação acessória. Malacarne e Camargo observam iniciativas voltadas a "identificar pesquisas, ferramentas e metodologias que proporcionam formas seguras de desenvolver sistemas" e apontam abordagens "que tratam desde vulnerabilidades da OWASP até métodos completos de desenvolvimento seguro" [Malacarne and Camargo 2021]. Como o aplicativo raramente funciona de forma isolada, APIs, serviços em nuvem, bibliotecas externas, mecanismos de autenticação e componentes de monitoramento ampliam os pontos de exposição e fazem com que o conteúdo percorra várias camadas. Por isso, uma leitura de riscos voltada a esse campo precisa considerar essas condições para identificar, com mais precisão, onde a informação pode ser exposta, utilizada indevidamente ou protegida de forma insuficiente.

3. Metodologia

Este estudo adota abordagem qualitativa e exploratória, baseada em revisão bibliográfica narrativa, de caráter não exaustivo, e em pesquisa documental. Godoy observa que, em pesquisas qualitativas, "um fenômeno pode ser melhor compreendido no contexto em que ocorre e do qual é parte" e destaca a análise em "perspectiva integrada" [Godoy 1995]. Piovesan e Temporini acrescentam que a pesquisa exploratória "apresenta natureza qualitativa e contextual" e contribui para "elaborar um instrumento de pesquisa adequado à realidade" [Piovesan and Temporini 1995]. O trabalho não testa relações causais nem compara experimentalmente métodos; seu objetivo é formular uma abordagem complementar de modelagem de ameaças em aplicativos móveis orientada à LGPD.

A etapa bibliográfica reuniu publicações relacionadas à LGPD, proteção de dados pessoais, modelagem de ameaças, segurança de software, privacidade e desenvolvimento móvel. Cavalcante e Oliveira registram que "os estudos de revisão bibliográfica caracterizam-se pelo uso e análise de documentos de domínio científico" e que "a pesquisa bibliográfica utiliza-se de fontes secundárias" [Cavalcante and de Oliveira 2020]. A pesquisa documental considerou legislação, guias oficiais e referências técnicas pertinentes ao tratamento de dados pessoais e à segurança de aplicativos. Godoy caracteriza esse procedimento como "o exame de materiais de natureza diversa, que ainda não receberam um tratamento analítico, ou que podem ser reexaminados, buscando-se novas e/ou interpretações complementares" [Godoy 1995]. As fontes foram priorizadas por sua aderência ao problema e por sua contribuição para a construção da proposta.

O corpus foi organizado em duas frentes complementares: literatura acadêmica sobre segurança, privacidade, proteção de dados, modelagem de ameaças e ambiente móvel; e documentos normativos e técnicos relacionados à LGPD e às práticas de proteção. A articulação dos conteúdos permitiu reunir elementos recorrentes sobre escopo, ativos, dados pessoais, fluxos, ameaças, controles e exigências normativas. Esses elementos foram organizados em quatro movimentos analíticos: delimitação da análise; identificação de ativos, dados pessoais e fluxos; identificação de ameaças; e correlação entre ameaças, controles e exigências da LGPD.

Por fim, a proposta foi submetida a uma avaliação conceitual estruturada no cenário *Mais Saúde*. O procedimento percorreu os quatro movimentos da abordagem

e considerou seis critérios. A cobertura foi examinada pela execução e pelas saídas de cada movimento; a rastreabilidade, pela ligação entre fluxo, ameaça, controle e LGPD; e o tratamento conjunto, pela presença de ameaças de segurança e privacidade. A avaliação também considerou as particularidades do ambiente móvel, a produção de registros estruturados e a continuidade entre as saídas de um movimento e as entradas do seguinte.

4. Estrutura analítica da abordagem orientada à LGPD

Esta seção sistematiza a proposta central do artigo. Sua contribuição está em organizar a modelagem de ameaças em aplicativos móveis por meio de uma estrutura analítica orientada à LGPD, capaz de aproximar pontos de tratamento de dados, ameaças identificadas e decisões técnicas de proteção.

A organização da proposta se dá em quatro movimentos sequenciais: delimitação da análise, identificação de ativos, dados pessoais e fluxos, identificação de ameaças e correlação entre ameaças, controles e exigências da LGPD. Em termos operacionais, esses movimentos respondem, em ordem, a quatro perguntas: o que deve ser analisado com prioridade, que elementos e fluxos precisam ser protegidos, que ameaças podem surgir nesse contexto e que respostas técnicas e normativas podem ser associadas a essas ameaças.

Os princípios de *Privacy by Design* e *Privacy by Default* orientam os quatro movimentos. A delimitação da análise expressa a proatividade ao priorizar operações em que finalidade, sensibilidade e exposição exigem maior atenção. O mapeamento de ativos, dados e fluxos incorpora a privacidade ao projeto e considera coleta, uso, armazenamento, compartilhamento e descarte. A identificação de ameaças mantém o caráter preventivo, enquanto a correlação com controles e LGPD favorece requisitos de minimização, restrição de acesso, limitação da retenção, transparência e proteção do conteúdo.

A Tabela 2 sintetiza o funcionamento da proposta. O exame parte da definição do recorte, passa pelo mapeamento dos elementos relevantes e pela identificação das ameaças e chega à correlação entre ameaça, medida de proteção e exigência da LGPD. A saída de cada movimento alimenta o seguinte e forma um encadeamento entre ponto de exposição, ameaça identificada, resposta técnica e fundamento normativo.

4.1. Delimitação da análise

O primeiro movimento estabelece o recorte da modelagem. Em sistemas móveis, essa etapa se torna necessária porque o tratamento de informações não se limita ao que aparece na interface principal. Permissões do sistema operacional, notificações, armazenamento local, comunicação com serviços remotos, rotinas em segundo plano e componentes integrados também participam desse processo. Sem uma delimitação inicial, a análise tende a perder foco e utilidade para decisões concretas de projeto.

Seu objetivo não é descrever exaustivamente todas as funcionalidades da solução, mas reconhecer onde o tratamento de dados pessoais assume maior relevância. Nesta proposta, o recorte é definido com base em três critérios. O primeiro é a relevância da informação manipulada, isto é, o grau de sensibilidade ou impacto associado a ela. O segundo é a criticidade do ponto em que ela é utilizada, ou seja, os locais da solução em que coleta, processamento, armazenamento ou compartilhamento ampliam a exposição. O terceiro é a distância entre a finalidade declarada e o comportamento efetivo da solução,

Tabela 2. Síntese da abordagem orientada à LGPD para modelagem de ameaças em aplicativos móveis

Movimento	Objetivo	Entrada	Saída esperada
Delimitação da análise	Definir o recorte da modelagem e priorizar pontos sensíveis do tratamento	Descrição funcional, permissões, integrações e recursos do dispositivo	Recorte priorizado dos pontos críticos de tratamento
Identificação de ativos, dados pessoais e fluxos	Mapear elementos relevantes à proteção e à circulação dos dados	Escopo definido	Mapa de ativos, categorias de dados e percursos informacionais
Identificação de ameaças	Identificar ameaças associadas às operações de tratamento e aos pontos de exposição	Ativos, dados e fluxos mapeados	Matriz de ameaças associadas a ativos e fluxos específicos
Correlação entre ameaças, controles e exigências da LGPD	Relacionar ameaças, respostas técnicas e fundamentos normativos aplicáveis	Ameaças identificadas	Cadeia de rastreabilidade entre ameaça, resposta técnica e exigência normativa

buscando identificar situações em que ela faz mais do que o usuário consegue perceber ou do que foi formalmente justificado.

Ao final desse movimento, obtém-se um recorte priorizado da solução, com indicação das operações e dos pontos críticos que devem ser aprofundados nas etapas seguintes. Esse resultado não pretende esgotar a descrição do aplicativo, mas orientar a atenção para os trechos em que o exame das ameaças se mostra mais necessário.

4.2. Identificação de ativos, dados pessoais e fluxos

Definido o recorte, o segundo movimento volta-se ao mapeamento dos elementos centrais da solução. Isso envolve identificar os ativos relevantes, as categorias de dados pessoais utilizadas e os percursos pelos quais esse conteúdo circula dentro e fora do aplicativo.

Nesta proposta, ativo não se restringe a um bem técnico isolado. O termo abrange elementos cujo comprometimento pode afetar segurança, privacidade ou conformidade, como credenciais, tokens de sessão, bases locais, interfaces de autenticação, serviços remotos, componentes de terceiros e mecanismos de armazenamento. Os dados pessoais, por sua vez, correspondem ao que é utilizado pelo aplicativo, a exemplo de dados cadastrais, identificadores, registros de uso, localização e, quando presentes, informações sensíveis, como dados de saúde. Já os percursos dizem respeito aos caminhos pelos quais

esse conteúdo é coletado, processado, armazenado, compartilhado ou descartado ao longo do funcionamento da solução.

A função dessa etapa é indicar não apenas o que existe na solução, mas o que requer proteção, quais categorias exigem maior atenção e em que pontos a circulação da informação amplia a exposição. Seu resultado esperado é um mapa de ativos, dados e fluxos capaz de sustentar a etapa seguinte, na qual esses elementos deixam de ser apenas descritos e passam a ser examinados à luz dos problemas que podem emergir de sua circulação.

4.3. Identificação de ameaças à segurança e à privacidade

Uma vez identificados os ativos, os dados utilizados e os percursos relevantes, o terceiro movimento consiste em reconhecer que problemas podem surgir a partir dessa circulação. O ponto central, aqui, não é listar ameaças de forma genérica, mas observar como cada percurso pode criar condições para exposição indevida, uso não autorizado, alteração, perda de confidencialidade ou utilização incompatível com a finalidade informada.

A passagem do mapeamento para a identificação das ameaças ocorre quando se examina de que modo a informação atravessa a solução e em que pontos esse trajeto se torna mais sensível. Se um dado permanece armazenado localmente, por exemplo, a leitura deve considerar possibilidades ligadas à manutenção excessiva, ao acesso indevido ou à proteção insuficiente. Quando ele é transmitido a serviços remotos, entram em cena problemas relacionados à interceptação, ao compartilhamento excessivo ou à ampliação desnecessária de seu alcance. Se o percurso envolve componentes de terceiros, também se deve observar a possibilidade de uso opaco, repasse sem necessidade clara ou perda de controle após deixar o aplicativo.

Em vez de tratar a ameaça de forma abstrata, a proposta procura indicar que ativo ou percurso está envolvido, que tipo de problema emerge desse contexto e por que ele é relevante para segurança, para privacidade ou para ambas. O resultado dessa etapa é uma matriz de ameaças associadas a pontos específicos da solução, funcionando como ponte entre o mapeamento anterior e a definição, na etapa seguinte, das respostas técnicas e normativas mais adequadas.

4.4. Correlação entre ameaças, controles e exigências da LGPD

O quarto movimento relaciona as ameaças identificadas às respostas técnicas e às exigências da LGPD que orientam seu tratamento. O objetivo, aqui, não é apenas registrar que um problema existe, mas explicitar que medida pode ser adotada diante dele e de que forma essa medida se conecta ao uso das informações envolvidas.

A correlação proposta segue um encadeamento simples. Primeiro, identifica-se em que ativo ou percurso a ameaça incide. Em seguida, define-se que resposta técnica pode reduzir sua ocorrência ou seu impacto. Por fim, observa-se que exigência da LGPD é tensionada por aquele problema e em que medida a solução escolhida ajuda a enfrentá-lo.

Se a ameaça decorre de coleta ou compartilhamento excessivo, por exemplo, a correlação tende a remeter à necessidade da informação e à limitação de seu alcance. Diante de exposição indevida, ganham importância medidas ligadas à proteção do armazenamento, da comunicação e do acesso. Quando a fragilidade envolve manutenção

do conteúdo por tempo superior ao necessário, torna-se preciso examinar critérios de retenção e descarte.

Essa etapa conclui o percurso analítico da abordagem. Seu resultado esperado é uma cadeia de rastreabilidade entre ameaça identificada, resposta técnica e exigência associada ao uso da informação. A modelagem passa, assim, a indicar não só onde está a ameaça, mas também por que determinada medida se mostra pertinente naquele contexto e que aspecto do tratamento realizado pelo aplicativo ela ajuda a qualificar. Com isso, reduz-se a distância entre o reconhecimento do problema e a definição de uma resposta, favorecendo decisões mais justificáveis e mais fáceis de rastrear ao longo do desenvolvimento.

5. Avaliação conceitual da abordagem no cenário *Mais Saúde*

A avaliação conceitual foi conduzida no cenário *Mais Saúde*, escolhido por reunir dados sensíveis, autenticação, armazenamento local, notificações e integrações externas. A Figura 1 representa os principais percursos informacionais utilizados na execução dos quatro movimentos e na análise dos critérios definidos na metodologia.

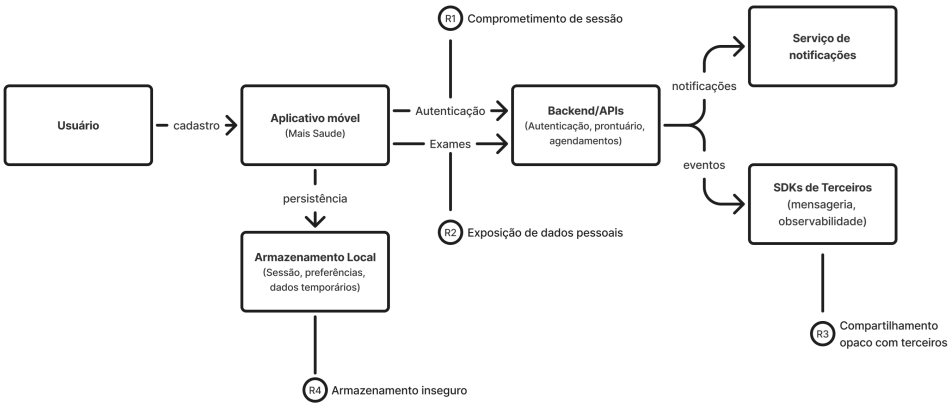

Figura 1. Visão geral do cenário conceitual do aplicativo *Mais Saúde*

O cenário considera a entrada de credenciais, a comunicação com serviços remotos, a permanência de dados no dispositivo, a exibição de notificações e o compartilhamento com componentes externos. Esses percursos permitem examinar como ativos e dados pessoais podem ser expostos durante a coleta, o uso, o armazenamento e a circulação.

5.1. Delimitação da análise no cenário

Entrada: descrição funcional do cenário, recursos do dispositivo, pontos de armazenamento e integrações externas. O primeiro movimento priorizou autenticação, armazenamento local, notificações e serviços de terceiros, por concentrarem dados sensíveis ou ampliarem sua exposição. O recorte não busca descrever todas as funcionalidades do aplicativo, mas selecionar os pontos em que o tratamento exige maior atenção.

Saída: conjunto priorizado de quatro pontos de tratamento, utilizado como entrada para o mapeamento dos ativos, dados e fluxos.

5.2. Ativos, dados e fluxos observados

Entrada: pontos priorizados no movimento anterior. No fluxo de autenticação, foram considerados credenciais, identificadores e artefatos de sessão transmitidos entre usuário, aplicativo e serviço remoto. No armazenamento local, foram observados dados de saúde e registros mantidos no dispositivo. Nas notificações, o conteúdo percorre o serviço remoto, o mecanismo do sistema operacional e a tela do dispositivo. Nas integrações externas, dados pessoais, identificadores técnicos e eventos de uso podem ser enviados a APIs, serviços analíticos, componentes de monitoramento ou outros provedores.

Saída: mapa conceitual dos ativos, categorias de dados e percursos informacionais, indicando onde o conteúdo é coletado, transmitido, armazenado, exibido ou compartilhado.

5.3. Ameaças identificadas no cenário

Entrada: ativos, dados e fluxos mapeados. O terceiro movimento examinou ameaças de segurança e privacidade associadas a cada percurso. No fluxo de autenticação, ameaças de segurança incluem uso indevido de credenciais e captura de sessão, enquanto a exposição desnecessária de identificadores também representa ameaça à privacidade. No armazenamento local, acesso indevido e proteção insuficiente correspondem a ameaças de segurança, ao passo que retenção excessiva e persistência sem necessidade decorrem da forma de tratamento dos dados.

Nas notificações, a exibição de informações em tela bloqueada pode produzir divulgação indevida e exposição fora do contexto esperado. Nas integrações externas, problemas de segurança podem decorrer de acesso ou transmissão inadequadamente protegidos, enquanto compartilhamento excessivo, uso opaco e perda de controle após deixar o aplicativo caracterizam ameaças à privacidade.

Saída: registro estruturado que relaciona cada ponto analisado ao ativo, ao fluxo, às ameaças identificadas e às possíveis respostas técnicas. Na Tabela 3, "S" representa segurança e "P" representa privacidade. A indicação de STRIDE, LINDDUN e PASTA registra formas possíveis de apoiar a identificação ou priorização das ameaças, sem pressupor a execução integral desses métodos.

5.4. Correlação entre ameaças, controles e LGPD

Entrada: ameaças relacionadas aos ativos e fluxos do cenário. O quarto movimento associou cada ameaça a uma resposta técnica e às exigências da LGPD tensionadas pelo tratamento. Na autenticação, a proteção não se limita ao canal, pois também envolve sessão, acesso e minimização dos identificadores. No armazenamento local, criptografia e controle de acesso precisam ser acompanhados da revisão da necessidade, do tempo de retenção e do descarte.

Nas notificações, a resposta considera não apenas a transmissão, mas também a visibilidade do conteúdo no dispositivo. Nas integrações externas, a proteção do canal deve ser combinada com minimização, limitação do compartilhamento, avaliação dos terceiros e transparência sobre a circulação dos dados.

Saída: cadeia de rastreabilidade entre ponto analisado, ativo, fluxo, ameaça, método de apoio, resposta técnica e exigência da LGPD. A Tabela 3 materializa essa saída em um registro que pode ser preenchido durante a análise de outros fluxos.

Tabela 3. Rastreabilidade da avaliação conceitual no cenário *Mais Saúde*

Ponto	Ativo e fluxo	Ameaça e natureza	Apoio	Resposta técnica	LGPD
Autenticação	Credenciais, identificadores e sessão entre aplicativo e serviço remoto	Uso indevido de credenciais ou captura de sessão (S); exposição desnecessária de identificadores (P)	STRIDE/ PASTA	Proteção do canal, autenticação fortalecida, proteção da sessão e minimização de identificadores	Segurança, prevenção e necessidade
Armazenamento local	Dados de saúde e registros mantidos no dispositivo	Acesso indevido ou proteção insuficiente (S); retenção ou persistência excessiva (P)	STRIDE/ LINDDUN	Criptografia local, restrição de acesso, minimização da persistência, retenção e descarte	Necessidade, segurança e limitação da conservação
Notificações	Conteúdo enviado pelo serviço remoto e exibido pelo sistema operacional	Divulgação em tela bloqueada (S); exposição fora do contexto esperado (P)	LINDDUN/ STRIDE	Conteúdo genérico, ocultação de dados sensíveis, controle de visibilidade e reautenticação	Adequação, prevenção e proteção contra divulgação indevida
Integrações externas	Dados pessoais e eventos enviados a APIs, serviços analíticos ou provedores	Acesso ou transmissão inadequados (S); compartilhamento excessivo, uso opaco ou perda de controle (P)	LINDDUN/ PASTA	Redução dos campos, restrição de acesso, proteção do canal, avaliação de terceiros e limitação do repasse	Finalidade, necessidade, transparência e segurança

A cobertura dos quatro movimentos pode ser observada na produção sucessiva do recorte, do mapa de ativos e fluxos, do registro de ameaças e da cadeia técnico-normativa. A rastreabilidade é examinada pela ligação entre fluxo, ameaça, controle e LGPD, enquanto o tratamento conjunto aparece na distinção entre ameaças de segurança e privacidade. As particularidades do ambiente móvel são representadas pelo armazenamento no dispositivo, pelas notificações, pela autenticação e pelas integrações externas. A estrutura tabular permite examinar a capacidade de operacionalização, e a continuidade entre as etapas permite analisar a coerência interna.

A avaliação permanece restrita a um único cenário conceitual, elaborado e examinado pelos próprios autores, o que pode introduzir circularidade entre a definição do caso e a aplicação da abordagem. Não houve avaliação independente, aplicação por equipes distintas, comparação estruturada com outros métodos ou mensuração quantitativa. As evidências permitem examinar cobertura, rastreabilidade, operacionalização e coerência interna, mas não sustentam conclusões sobre completude, desempenho ou generalização para outros sistemas e domínios.

6. Discussão

STRIDE, LINDDUN e PASTA possuem escopos distintos e são tratados neste artigo como referências complementares. A proposta não reproduz suas taxonomias ou procedimentos; organiza seus possíveis resultados em um percurso que relaciona particularidades do ambiente móvel, controles técnicos e exigências da LGPD.

Esse percurso também aproxima a proposta de *Privacy by Design* e *Privacy by Default*. A proteção é considerada desde a delimitação do escopo e o mapeamento dos fluxos. A identificação antecipada de ameaças expressa o caráter preventivo, enquanto a correlação com controles favorece minimização dos dados, limitação da retenção, restrição do compartilhamento e redução da exposição em notificações. A rastreabilidade entre fluxo, ameaça, controle e LGPD torna as decisões de proteção mais explícitas e justificáveis.

A avaliação conceitual no cenário *Mais Saúde* permitiu observar a cobertura dos quatro movimentos, a continuidade entre suas entradas e saídas e a produção de registros que relacionam ativos, fluxos, ameaças, controles e exigências normativas. A distinção entre ameaças de segurança e privacidade mostrou que um mesmo ponto pode envolver problemas diferentes. O armazenamento local, por exemplo, pode apresentar acesso indevido e proteção insuficiente, mas também retenção excessiva. As integrações externas podem envolver comunicação inadequadamente protegida e, simultaneamente, compartilhamento excessivo ou uso opaco dos dados. Autenticação, armazenamento no dispositivo, notificações e serviços externos também permitiram examinar particularidades do ambiente móvel.

Para a Engenharia de Software, a abordagem oferece uma estrutura que pode apoiar a transformação das ameaças identificadas em requisitos de segurança e privacidade, decisões arquiteturais, critérios de revisão e registros de rastreabilidade. Para a proteção de dados, aproxima princípios normativos dos pontos concretos em que a informação é coletada, transmitida, armazenada, exibida ou compartilhada. Seu valor está menos na identificação de ameaças inéditas e mais na integração entre dimensões técnicas e normativas frequentemente tratadas de forma separada.

Essas limitações restringem os resultados à cobertura, à rastreabilidade, à operacionalização e à coerência interna do cenário analisado. Portanto, não permitem inferir completude, desempenho ou generalização para outros sistemas e domínios.

7. Conclusão

Este artigo teve como objetivo propor uma abordagem complementar de modelagem de ameaças para aplicativos móveis orientada à LGPD. Sua contribuição central consiste na organização de quatro movimentos que relacionam delimitação do escopo, ativos e fluxos de dados pessoais, ameaças de segurança e privacidade, controles técnicos e exigências normativas.

A avaliação conceitual no cenário *Mais Saúde* permitiu observar que a estrutura organiza uma cadeia de rastreabilidade entre ponto de exposição, ameaça, resposta técnica e LGPD, além de considerar particularidades do ambiente móvel, como autenticação, armazenamento local, notificações e integrações externas. O principal resultado conceitual está na indicação de que métodos consolidados podem apoiar a identificação das ameaças, enquanto a proposta organiza seus possíveis resultados em uma perspectiva técnico-normativa.

O estudo permanece restrito ao exame conceitual de um cenário elaborado pelos próprios autores e não contou com avaliação independente ou comparação estruturada com outras abordagens. Trabalhos futuros devem examinar a proposta com equipes distintas, em diferentes domínios, e desenvolver artefatos de apoio, como modelos, listas de verificação e critérios de priorização, para analisar sua compreensão, repetibilidade e utilidade ao longo do ciclo de desenvolvimento.

Referências

Alves, L. F., Amalfi, P., Martin, S., Schepke, C., Rodrigues, E., and Bernardino, M. (2024). Modelagem de ameaças com stride e dread. In *Escola Regional de Engenharia de Software*, E-RES. Sociedade Brasileira de Computação. Acesso em: 26 jul. 2026.

Andrade, A. W., Agra, R., and Malheiros, V. (2013). Estudos de caso de aplicativos móveis no governo brasileiro. In *Anais do Simpósio Brasileiro de Sistemas de Informação*, SBSI, pages 780–791, João Pessoa. Sociedade Brasileira de Computação. Acesso em: 26 jul. 2026.

Brasil (2018). Lei geral de proteção de dados pessoais – lgpd. `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm`. Acesso em: 26 jul. 2026.

Cavalcante, L. T. C. and de Oliveira, A. A. S. (2020). Métodos de revisão bibliográfica nos estudos científicos. *Psicologia em Revista*, 26(1):82–100.

Cerqueira, D. A., de Mello, R. M., and Travassos, G. H. (2023). Um checklist para inspeção de privacidade e proteção de dados pessoais em artefatos de software. In *Anais do XXVI Congresso Ibero-Americano em Engenharia de Software*, pages 206–213. Sociedade Brasileira de Computação.

De França, R. P. and Da Silva, V. B. (2022). Devsecops – integração da segurança contínua em pipelines devops: um estudo de caso. In *Anais do Workshop de Trabalhos de Iniciação Científica e de Graduação – Simpósio Brasileiro de Cibersegurança (SBSeg)*, pages 272–285, Porto Alegre. Sociedade Brasileira de Computação.

de Moura, L. V. and Coutinho, E. (2024). Lgpd e requisitos de software: Desafios e oportunidades de pesquisa. In *Anais do IX Workshop sobre Aspectos Sociais, Humanos e Econômicos de Software*, WASHES, pages 169–174. Sociedade Brasileira de Computação.

de Sá, M. D. (2019). Análise do impacto da nova lei de proteção de dados pessoais: estudo de caso com aplicativos móveis do governo. Documento de pós-graduação, Universidade Federal de Minas Gerais. Acesso em: 26 jul. 2026.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32.

European Union Agency for Cybersecurity (ENISA) (2022). Data protection engineering: From theory to practice. Technical report, European Union Agency for Cybersecurity (ENISA), Athens, Greece. Acesso em: 26 jul. 2026.

Ferreira, R. L. D. M., dos Santos, A. F. P., and Choren, R. (2017). Uma técnica prognóstica para desenvolvimento seguro de aplicativo android. *Journal on Advances in Theoretical and Applied Informatics*, 3(1):39–46.

Godoy, A. S. (1995). Pesquisa qualitativa: tipos fundamentais. *RAE - Revista de Administração de Empresas*, 35(3):20–29.

Jardim, G. P. S., Rabello, M. E. R., Lima, A. C., Brefeld, U., and Reis, V. Q. (2022). Uma caracterização das políticas de privacidade utilizadas em aplicativos no brasil. In *Anais do III Workshop sobre as Implicações da Computação na Sociedade*, WICS, pages 13–25. Sociedade Brasileira de Computação.

Malacarne, G. R. and Camargo, E. T. (2021). Desenvolvimento seguro de sistemas web: uma revisão sistemática. In *Escola Regional de Engenharia de Software*, ERES, pages 1–10, Porto Alegre. Sociedade Brasileira de Computação. Acesso em: 26 jul. 2026.

Marques, T. C. and Santana, A. C. (2023). Segurança da informação aplicada em dispositivos móveis com foco na tecnologia bluetooth. *Latin American Journal of Development*, 5(3):881–892. Acesso em: 26 jul. 2026.

Microsoft (2023). Threats – microsoft threat modeling tool. Microsoft Learn. Acesso em: 26 jul. 2026.

Oliveira, A. C. R., Ferreira, H. C., and Pires, F. I. (2021). Princípios da lei geral de proteção de dados (lgpd). *Seara Jurídica*, 22(59):431–446.

Piovesan, A. and Temporini, E. R. (1995). Pesquisa exploratória: procedimento metodológico para o estudo de fatores humanos no campo da saúde pública. *Revista de Saúde Pública*, 29(4):318–325.

Rodrigues, A., Villela, M. L., and Feitosa, E. (2023). Linguagem para a modelagem de ameaças de privacidade. In *Anais Estendidos do Simpósio Brasileiro sobre Fatores Humanos em Sistemas Computacionais*, volume 22 of *IHC*, pages 251–255, Maceió/AL, Brasil. Sociedade Brasileira de Computação.

Santos, L. C. M. d. C., Prado, E. P. V., and Chaim, M. L. (2020). Técnicas e ferramentas para detecção de vulnerabilidades em ambientes de desenvolvimento ágil de software. *Brazilian Journal of Development*, 6(6):33921–33941.

Silva, A. V. d., Rosa, P. V. G., Ferneda, E., and Braga Filho, M. d. O. (2018). Utilização e compartilhamento de dados capturados por aplicativos de smartphones: uma revisão sistemática de literatura. *Revista GCTI*, 4(1):21–48.

Teffé, C. S. d. and Viola, M. (2020). Tratamento de dados pessoais na lgpd: estudo sobre as bases legais para o tratamento de dados pessoais na lei geral de proteção de dados brasileira (lgpd – lei n. 13.709/18). *Civilística*, 9(1):1–24.

UcedaVelez, T. and Morana, M. M. (2015). *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons.