UNIVERSIDADE FEDERAL DE PERNAMBUCO
CURSO DE SISTEMAS DE INFORMAÇÃO
CENTRO DE INFORMÁTICA TRABALHO DE
CONCLUSÃO DE CURSO

EVOLUINDO O PRIVACY CRITERIA METHOD COM A MODELAGEM DE AMEAÇAS DE PRIVACIDADE DO MÉTODO LINDDUN E AS ESTRATÉGIAS DE MITIGAÇÃO DO MÉTODO STRIDE

MARCSON SILVA DOS SANTOS

Recife
2025

Marcson Silva dos Santos

EVOLUINDO O PRIVACY CRITERIA METHOD COM A MODELAGEM DE AMEAÇAS DE PRIVACIDADE DO MÉTODO LINDDUN E AS ESTRATÉGIAS DE MITIGAÇÃO DO MÉTODO STRIDE

Trabalho de Conclusão de Curso, apresentado ao Curso de Sistema de Informações da Universidade Federal de Pernambuco, como parte das exigências para obtenção do título de graduado.

Orientador(a): Carla Taciana Lima Lourenço Silva Schuenemann
Co-orientadora: Mariana Maia Peixoto

Recife

2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Santos, Marcson Silva dos.
Evoluindo o privacy criteria method com a modelagem de ameaças de privacidade do método LINDDUN e as estratégias de mitigação do método STRIDE / Marcson Silva dos Santos. - Recife, 2025.
66 p. : il., tab.

Orientador(a): Carla Taciana Lima Lourenço Silva Schuenemann
Cooorientador(a): Mariana Maia Peixoto
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2025.
Inclui referências.

1. Privacidade. 2. Segurança. 3. Requisitos. 4. Sistemas. 5. Mitigação de Ameaças. I. Schuenemann, Carla Taciana Lima Lourenço Silva. (Orientação). II. Peixoto, Mariana Maia. (Coorientação). IV. Título.

000 CDD (22.ed.)

MARCSON SILVA DOS SANTOS

EVOLUINDO O PRIVACY CRITERIA METHOD COM A MODELAGEM DE AMEAÇAS DE PRIVACIDADE DO MÉTODO LINDDUN E AS ESTRATÉGIAS DE MITIGAÇÃO DO MÉTODO STRIDE

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de bacharel em Sistemas de Informação.

Aprovado em: 07/10/2025

BANCA EXAMINADORA

Profa. Dra. Carla Taciana Lima Lourenço Silva Schuenemann

Universidade Federal de Pernambuco

Profa. Dra. Jéssyka Flavyanne Ferreira Vilela

Universidade Federal de Pernambuco

SUMÁRIO

RESUMO

A crescente digitalização dos serviços e a intensificação do uso de dados pessoais aumentaram os desafios relacionados à privacidade e à conformidade legal. As regulamentações, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e o General Data Protection Regulation (GDPR), definiram diretrizes rigorosas para a coleta, armazenamento e processamento de informações pessoais, exigindo que os sistemas fossem concebidos com mecanismos de proteção desde sua concepção. Apesar de as abordagens tradicionais da Engenharia de Requisitos, como casos de uso e histórias de usuários, serem eficazes para capturar requisitos funcionais e não funcionais, elas não são completamente adequadas para lidar com os desafios específicos de privacidade. De acordo com o estado da arte, a privacidade exige abordagens estruturadas e específicas, pois as metodologias tradicionais não oferecem uma análise aprofundada dos riscos. Isso torna necessário o uso de métodos que proporcionam uma análise mais detalhada dos riscos à privacidade e segurança desde as fases iniciais do desenvolvimento. O Privacy Criteria Method (PCM) é uma metodologia estruturada para identificar e mitigar riscos de privacidade nas fases iniciais do desenvolvimento de sistemas. Embora eficaz, o PCM apresenta limitações importantes, especialmente no que diz respeito à modelagem de ameaças e à validação da conformidade legal. Estas limitações tornam o método menos robusto, principalmente quando se trata de avaliar e integrar ameaças complexas que podem afetar a privacidade em sistemas modernos. Uma dessas limitações é a falta de uma abordagem específica para modelagem de ameaças à privacidade, o que pode resultar em uma avaliação incompleta dos riscos. Para superar essas deficiências, este trabalho propõe a integração do PCM com outras metodologias complementares, como LINDDUN e STRIDE. O LINDDUN é uma técnica focada especificamente nas ameaças relacionadas à privacidade, como linkability, identifiability e disclosure of information, aspectos cruciais para garantir a privacidade dos dados pessoais em sistemas. Por outro lado, o STRIDE é uma metodologia amplamente utilizada na modelagem de ameaças à segurança da informação, que abrange vulnerabilidades como spoofing, tampering e elevation of privilege, e que também impactam diretamente a privacidade dos usuários. A integração dessas metodologias com o PCM permite uma abordagem mais holística, oferecendo uma análise aprofundada tanto dos riscos de privacidade quanto das ameaças à segurança que podem comprometê-la. O LINDDUN adiciona uma camada essencial de proteção focada na privacidade, enquanto o STRIDE complementa o PCM ao abordar ameaças de segurança que, muitas vezes, não são consideradas no contexto da privacidade, mas têm um impacto direto sobre ela. Dessa forma, a combinação do PCM com LINDDUN e STRIDE resulta em um

framework mais completo, capaz de fornecer uma análise detalhada, mitigar riscos e garantir a conformidade legal de maneira mais eficaz. A combinação dessas técnicas aprimora o PCM ao fornecer diretrizes mais abrangentes para o desenvolvimento de sistemas que atendam às regulamentações, reduzam ameaças e protejam dados pessoais. Além disso, a metodologia proposta detalha um processo estruturado para implementação e validação de soluções de privacidade, auxiliando desenvolvedores na conformidade com LGPD e GDPR. O método proposto detecta riscos desde as fases iniciais do desenvolvimento e facilita a aplicação de mecanismos eficazes, assegurando confidencialidade, integridade e disponibilidade dos dados. A validade da abordagem foi confirmada por meio dos resultados obtidos a partir dos artefatos desenvolvidos pelos alunos, que demonstraram como a integração do PCM com LINDDUN e STRIDE fortalece a proteção dos dados assegurando ainda mais conformidade legal. Esses artefatos proporcionaram evidências de que a combinação das metodologias oferece uma análise mais detalhada e mais assertiva na identificação e mitigação de riscos à privacidade e segurança, favorecendo a criação de sistemas que atendam aos requisitos de privacidade e segurança de maneira mais robusta. Dessa forma, este trabalho contribui para a Engenharia de Requisitos, proporcionando um modelo que, ao integrar as modelagens, auxilia no desenvolvimento de sistemas mais alinhados às regulamentações vigentes. Embora a abordagem tenha mostrado resultados promissores, ela não oferece uma garantia absoluta, mas sim uma forma mais estruturada de tratar os requisitos de privacidade e segurança durante o ciclo de desenvolvimento.

Palavras-chave: Privacidade. Segurança. Dados. Requisitos. Sistemas. Mitigação de Ameaças.

ABSTRACT

The increasing digitalization of services and the intensification of the use of personal data have increased the challenges related to privacy and legal compliance. Regulations, such as the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR), have defined strict guidelines for the collection, storage, and processing of personal information, requiring systems to be designed with protection mechanisms from their inception. Although traditional Requirements Engineering approaches, such as use cases and user stories, are effective in capturing functional and non-functional requirements, they are not completely adequate to address specific privacy challenges. According to the state of art, privacy requires structured and specific approaches, as traditional methodologies do not offer an in-depth analysis of risks. This makes it necessary to use methods that provide a more detailed analysis of privacy and security risks from the early stages of development. The Privacy Criteria Method (PCM) is a structured methodology for identifying and mitigating privacy risks in the early stages of system development. Although effective, PCM presents important limitations, especially with regard to threat modeling and legal compliance validation. These limitations make the method less robust, especially when it comes to assessing and integrating complex threats that may affect privacy in modern systems. One of these limitations is the lack of a specific approach to privacy threat modeling, which may result in an incomplete risk assessment. To overcome these shortcomings, this work proposes the integration of PCM with other complementary methodologies, such as LINDDUN and STRIDE. LINDDUN is a technique specifically focused on privacy-related threats, such as linkability, identifiability, and disclosure of information, crucial aspects to guarantee the privacy of personal data in systems. On the other hand, STRIDE is a methodology widely used in information security threat modeling, which covers vulnerabilities such as spoofing, tampering, and elevation of privilege, and which also directly impact user privacy. The integration of these methodologies with PCM enables a more holistic approach, offering an in-depth analysis of both privacy risks and security threats that may compromise it. LINDDUN adds an essential layer of privacy-focused protection, while STRIDE complements PCM by addressing security threats that are often not considered in the context of privacy but have a direct impact on it. In this way, the combination of PCM with LINDDUN and STRIDE results in a more complete framework, capable of providing detailed analysis, mitigating risks and ensuring legal compliance more effectively. The combination of these techniques enhances PCM by providing more comprehensive guidelines for the development of systems that comply with regulations, reduce

threats and protect personal data. In addition, the proposed methodology details a structured process for implementing and validating privacy solutions, assisting developers in complying with LGPD and GDPR. The proposed method detects risks from the early stages of development and facilitates the application of effective mechanisms, ensuring confidentiality, integrity and availability of data. The validity of the approach was confirmed by the results obtained from the artifacts developed by the students, which demonstrated how the integration of PCM with LINDDUN and STRIDE strengthens data protection, ensuring even greater legal compliance. These artifacts provided evidence that the combination of methodologies offers a more detailed and assertive analysis in identifying and mitigating privacy and security risks, favoring the creation of systems that meet privacy and security requirements in a more robust manner. Thus, this work contributes to Requirements Engineering, providing a model that, by integrating the models, helps in the development of systems that are more aligned with current regulations. Although the approach has shown promising results, it does not offer an absolute guarantee, but rather a more structured way of dealing with privacy and security requirements during the development cycle.

Keywords: Privacy. Security. Data. Requirements. Systems. Threat Mitigation.

1. INTRODUÇÃO

1.1 Contexto

A crescente digitalização da sociedade tem impulsionado um uso intensivo de dados pessoais em diversas áreas, abrangendo desde plataformas de e-commerce e serviços de streaming até serviços de saúde, aplicativos de mobilidade urbana, assistentes virtuais e sistemas bancários digitais. No entanto, essa disseminação de dados traz desafios significativos para garantir a privacidade dos indivíduos e proteger suas informações contra acessos indevidos, vazamentos e usos não autorizados. A privacidade não se resume apenas ao controle sobre as informações pessoais, mas também ao respeito às normas que governam seu fluxo em diferentes contextos, sendo essencial considerar as especificidades de cada ambiente digital (Nissenbaum, 2004).

Assim, a privacidade tornou-se um aspecto essencial na Engenharia de Requisitos, demandando abordagens estruturadas para a especificação e mitigação de riscos no desenvolvimento de software (Peixoto, 2021). Para isso, é necessário que os sistemas sejam projetados com mecanismos adequados de proteção desde sua concepção, garantindo a segurança dos dados pessoais e a confiança dos usuários (Menegazzi, 2023).

Leis como o Regulamento Geral sobre a Proteção de Dados (GDPR) (GDPR.EU, 2018), na União Europeia, e a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018), no Brasil, estabelecem diretrizes para a coleta, armazenamento e compartilhamento de dados pessoais, exigindo que sistemas sejam projetados desde sua concepção com mecanismos adequados para garantir conformidade legal. Essas regulamentações trouxeram desafios adicionais para empresas e desenvolvedores, que precisam implementar mecanismos de privacidade eficazes e demonstrar conformidade contínua com as normas vigentes. A falta de abordagens estruturadas para lidar com requisitos de privacidade pode resultar em falhas de segurança, perda de confiança dos usuários e penalidades severas por descumprimento das leis.

Nesse cenário, a Engenharia de Requisitos surge como uma área essencial dentro do desenvolvimento de software, propondo técnicas e metodologias para especificar, analisar e validar requisitos de privacidade ao longo do ciclo de vida do sistema. Técnicas tradicionais de Engenharia de Requisitos, como casos de uso, histórias de usuário e modelagem de requisitos baseada em cenários, historicamente focam em aspectos funcionais e não funcionais gerais, mas às vezes não são suficientes para capturar a complexidade dos desafios impostos pelas regulamentações de privacidade.

Essas abordagens, embora eficientes na definição de requisitos de software, nem sempre abordam de maneira explícita aspectos cruciais para a proteção da privacidade, como a minimização de dados, o consentimento explícito e a proteção contra rastreamento. Tais aspectos são fundamentais para garantir conformidade com regulamentações como a GDPR e a LGPD, que exigem um enfoque mais detalhado e estruturado sobre a privacidade dos usuários desde a concepção do sistema. Como enfatizam autores como Nissenbaum (2004) e Peixoto (2021), a privacidade não deve ser tratada apenas como um requisito técnico, mas como um princípio fundamental que orienta todas as fases do desenvolvimento. Além disso, a crescente complexidade das leis de privacidade exige a adoção de métodos específicos que ajudem os desenvolvedores a identificar, documentar e implementar requisitos de privacidade de maneira eficaz e sistemática (Menegazzi, 2023).

1.2 Problema De Pesquisa

Dentre as abordagens existentes, o Método de Critérios de Privacidade (do inglês, Privacy Criteria Method - PCM) de Peixoto (2021), destaca-se como um método estruturado voltado para a especificação de requisitos de privacidade, oferecendo diretrizes para identificar e mitigar riscos de privacidade desde as primeiras fases do desenvolvimento. No entanto, embora o PCM seja uma ferramenta útil para auxiliar na definição desses requisitos, a metodologia ainda carece de um processo detalhado para apoiar a implementação da análise aprofundada dos cenários de risco e dos mecanismos de privacidade adequados para mitigá-los.

A integração do PCM com abordagens de análise de ameaças, como LINDDUN (Van Landuyt; Joosen, 2020) e STRIDE (Hossain; Hassan, 2023), pode ampliar sua eficácia ao fornecer uma estrutura que não apenas identifica riscos de privacidade, mas também considera ameaças de segurança que podem comprometer a proteção dos dados.

A pesquisa realizada neste trabalho visa preencher a lacuna na identificação de cenários de risco e mecanismos de privacidade ao propor uma melhoria no PCM, integrando-o a técnicas reconhecidas de modelagem de ameaças e especificação de mecanismos de privacidade. O objetivo é fornecer um método mais robusto que não apenas auxilie na definição dos requisitos de privacidade, mas também direcione sua implementação de forma prática, garantindo a conformidade legal e a proteção adequada dos dados pessoais dos usuários.

Além disso, a evolução do PCM com a integração das abordagens LINDDUN e STRIDE possibilita uma análise completa das ameaças de privacidade e vulnerabilidades de segurança associadas ao tratamento de dados pessoais. Enquanto o LINDDUN permite identificar ameaças à privacidade sob uma ótica estruturada e orientada a riscos, o STRIDE adiciona elementos de

mitigação de ameaças de segurança ao processo, permitindo que desenvolvedores avaliem e evitem ataques potenciais que podem comprometer a privacidade dos usuários.

Essa combinação cria um arcabouço metodológico promissor, auxiliando organizações e pessoas a não apenas atender às exigências regulatórias, mas também a implementar sistemas mais confiáveis e resilientes contra ameaças à privacidade e segurança dos dados.

1.3 Objetivos

1.3.1 Objetivo Geral

- Analisar e aprimorar a especificação de riscos e mecanismos de privacidade do PCM, propondo sua integração com os métodos LINDDUN e STRIDE para fortalecer a abordagem de segurança e privacidade.

1.3.2 Objetivos Específicos

- Analisar a compatibilidade do PCM com os métodos STRIDE e LINDDUN, avaliando como essas técnicas podem complementar sua abordagem na identificação e mitigação de ameaças à privacidade.
- Propor uma integração estruturada do PCM com STRIDE e LINDDUN, fornecendo diretrizes para fortalecer a análise de riscos e a definição de mecanismos de privacidade no desenvolvimento de software.

1.4 Método De Pesquisa

Este estudo caracteriza-se como uma pesquisa metodológica, exploratória e descritiva, com aplicação ilustrativa baseada em análise de documentos secundários. Segundo Gil (2017, p. 44), a pesquisa exploratória visa proporcionar maior familiaridade com o problema, tornando-o mais explícito ou ajudando a construir hipóteses. No contexto deste trabalho, essa abordagem é utilizada para investigar a viabilidade da integração dos métodos STRIDE e LINDDUN ao Privacy Criteria Method (PCM), analisando sua compatibilidade conceitual e funcional.

Além disso, este estudo possui um caráter descritivo, pois visa apresentar de forma detalhada como os métodos podem ser incorporados ao PCM. De acordo com Gil (2017, p. 45), a pesquisa descritiva tem como principal finalidade "descrever as características de determinada

população ou fenômeno", permitindo compreender melhor os aspectos envolvidos na aplicação dos métodos STRIDE e LINDDUN.

Tal definição encontra respaldo na afirmação de Severino (2017) de que a pesquisa descritiva visa registrar, analisar, classificar e interpretar fenômenos observados, sem que o pesquisador interceda diretamente, conforme a proposta deste estudo e que a pesquisa exploratória e descritiva deste trabalho são de fato, metodologicamente, fundamentadas no que dizem Marconi e Lakatos (2017, p. 169), no sentido de que a pesquisa descritiva é insubstituível para a caracterização dos fenômenos e para a compreensão de suas particularidades, assim como a pesquisa exploratória possui uma função investigativa indispensável na construção de novos conhecimentos.

Para conduzir este estudo, inicialmente foi realizada uma análise exploratória do PCM, avaliando suas limitações na modelagem de ameaças e conformidade legal. Em seguida, foram conduzidos estudos ilustrativos para demonstrar a aplicabilidade do PCM em cenários reais. Com base nesses estudos, propôs-se a integração do PCM com os métodos LINDDUN e STRIDE, aprimorando a identificação e mitigação de riscos à privacidade e à segurança.

Posteriormente, a proposta foi avaliada através da análise de artefatos produzidos por alunos, os quais aplicaram o PCM e LINDDUN em um exemplo ilustrativo. A avaliação desses artefatos foi estruturada na seção 5.1 e 5.2, que define critérios de qualidade para verificar a correta aplicação das metodologias e sua eficácia na especificação de requisitos de privacidade.

1.4.1 Estratégia metodológica: Análise teórico-exploratória baseada em exemplos

Esta pesquisa adota uma abordagem metodológica teórico-exploratória, utilizando o cenário de uma paciente de uma clínica chamada Alice, descrito por Peixoto (2021), como base para avaliar conceitualmente a integração dos métodos STRIDE e LINDDUN ao PCM. Diferentemente de uma pesquisa experimental tradicional, que requer manipulação direta de variáveis em condições controladas (GIL, 2017), este estudo não envolve intervenção direta no fenômeno observado. Em vez disso, realiza-se uma análise de artefatos de especificação, permitindo uma avaliação teórica.

Segundo Casarin e Casarin (2012), esse tipo de investigação é voltado para a formulação de conceitos, hipóteses e modelos teóricos, com base em dados documentais ou observações indiretas. Em complemento, Wainer et al. (2007) reforçam que, no campo da ciência da computação, análises exploratórias são essenciais para investigar fenômenos emergentes e ainda pouco estruturados, permitindo a construção gradual de conhecimento a partir da realidade observada. Mais recentemente, Wagner et al. (2019) destacam que a pesquisa exploratória é útil para esclarecer conceitos, estabelecer

prioridades de investigação e identificar variáveis relevantes, especialmente em estudos que envolvem aspectos técnicos e sociais como privacidade e segurança da informação.

1. **Revisão Bibliográfica**
    - Leitura aprofundada sobre as metodologias STRIDE, LINDDUN;
    - Estudo de obras referenciais em metodologia científica;
    - Identificação das lacunas metodológicas no PCM e fundamentação teórica da integração com os outros métodos.
2. **Análise Documental Exploratória**
    - Utilização do estudo clínico de Alice, conforme descrito por Peixoto (2021);
    - Extração das informações relevantes para aplicação do PCM;
    - Interpretação crítica dos elementos de privacidade e segurança no contexto analisado.
3. **Integração com LINDDUN e STRIDE**
    - Proposição de uma integração conceitual e funcional entre PCM, STRIDE e LINDDUN;
    - Definição de fluxos e diretrizes para orientar a análise de riscos de privacidade e segurança.
4. **Estudo Ilustrativo Complementar**
    - Aplicação da proposta em artefatos desenvolvidos por alunos em contextos simulados de Engenharia de Requisitos;
    - Avaliação qualitativa da aplicação das metodologias com base em critérios de clareza, conformidade legal e aplicabilidade técnica.
5. **Avaliação e Discussão dos Resultados**
    - Comparação dos resultados obtidos com os objetivos definidos;
    - Reflexão crítica sobre a eficácia da integração proposta e suas limitações.

1.4.2 Ameaças à validade

Como qualquer estudo acadêmico, esta pesquisa apresenta algumas limitações que devem ser consideradas ao interpretar seus resultados. Primeiramente, a principal limitação está na ausência de testes empíricos para validar a eficácia da integração dos métodos STRIDE e LINDDUN ao Privacy Criteria Method (PCM). Embora a aplicação teórica desses métodos tenha sido realizada de forma sistemática e fundamentada, não foram conduzidos experimentos práticos ou avaliações quantitativas para medir sua eficiência na mitigação de ameaças à segurança e privacidade em um ambiente real de desenvolvimento de software.

Outra limitação relevante está na dependência de um exemplo de ilustração preexistente. O caso da paciente Alice, descrito na tese de Peixoto (2021), serviu como base documental para a aplicação conceitual das modelagens. Além disso, a análise realizada nesta pesquisa incluiu artefatos desenvolvidos pelos alunos da disciplina de Engenharia de Requisitos (2024.2) do curso de Sistemas de Informação.

Foram avaliados 17 artefatos, com base nos critérios de qualidade estabelecidos na Seção 5, permitindo uma primeira avaliação da aplicabilidade da modelagem proposta. No entanto, essa análise apresenta algumas ameaças à validade, como a variação na experiência dos alunos com modelagem de ameaças e requisitos de privacidade, o que pode ter impactado a aplicação correta da metodologia.

Ademais, a ausência de um ambiente controlado e a subjetividade na interpretação dos critérios de avaliação podem ter influenciado os resultados. Para mitigar essas limitações, recomenda-se a realização de testes complementares em um ambiente profissional, envolvendo especialistas em segurança e privacidade, a fim de avaliar a aplicabilidade prática da modelagem proposta. A aplicação da abordagem em sistemas reais e variados, como ambientes corporativos, governamentais e de saúde, pode fornecer uma visão mais abrangente de sua eficácia, permitindo ajustes e refinamentos para garantir sua robustez.

A realização de simulações controladas e a definição de métricas quantitativas possibilita uma avaliação mais objetiva do impacto da modelagem na mitigação de ameaças à segurança e proteção de dados. Por fim, a coleta de feedback de especialistas e desenvolvedores, por meio de entrevistas ou questionários, contribuiria para validar a usabilidade e aceitação dessa abordagem no mercado, garantindo maior confiabilidade e adaptação da metodologia a diferentes cenários de aplicação.

Diante dessas limitações, esta pesquisa deve ser vista como um ponto de partida para investigações futuras, que podem envolver avaliações experimentais, aplicação prática em projetos reais e análise comparativa com outras metodologias. Assim, os resultados aqui apresentados contribuem para a construção de um arcabouço teórico para a melhoria da segurança e privacidade no desenvolvimento de software, mas demandam aprofundamento para sua completa validação e aplicabilidade prática.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Privacidade

Privacidade é o poder do indivíduo controlar o que as pessoas podem ou não saber sobre ele e, portanto, guardar suas informações em segredo e sem intromissão de terceiros (Warren; Brandeis, 1890). Além disso, a privacidade não somente é controle sobre as informações pessoais, mas também respeito às normas que governam o fluxo de informações em cada contexto, quando os princípios não seguidos, integralmente, a privacidade é violada (Nissenbaum; Helen, 2004).

Segundo Alan Westin (1968) a privacidade é definida como a reivindicação de indivíduos, grupos ou instituições de controle quando, como e em que medida suas informações são comunicadas a terceiros. Essa perspectiva enfatiza a autonomia individual sobre as informações pessoais (Peixoto, 2021). Desse modo, as práticas de privacidade devem assegurar que os dados sejam utilizados exclusivamente para os fins pretendidos, permitindo que os indivíduos tomem decisões sobre o uso de suas informações (Menegazzi, 2023).

Conforme a Organização para a Cooperação e Desenvolvimento Econômico (2025), visando à proteção das informações coletadas na era digital, foram criadas as diretrizes que possuem os objetivos de proteger a privacidade e os dados pessoais. Sendo assim, a responsabilidade dos controladores de dados deverá ter preponderância, com o auxílio da cooperação internacional, para que as legislações do direito se harmonizem e se obtenha mais eficácia no tratamento dos fluxos transfronteiriços de dados. Esses princípios visam equilibrar a proteção da privacidade das pessoas e o crescimento econômico e social mundial.

Além disso, para garantir com mais afinco a privacidade durante o desenvolvimento de softwares deve-se aplicar a Privacidade por Design (do inglês, Privacy by Design - PbD) desde o início da criação, que consta na Regulamento Geral sobre a Proteção de Dados (GDPR), para que aplicação ocorra de forma efetiva todas as partes envolvidas de forma ativa no desenvolvimento dos sistemas (Martin; Kung, 2018).

2.2 Segurança

A segurança da informação fundamenta-se na tríade de Confidencialidade, Integridade e Disponibilidade (CID), princípios essenciais para a proteção de sistemas e dados sensíveis. A confidencialidade assegura que as informações sejam acessadas apenas por usuários autorizados, prevenindo acessos indevidos e vazamentos de dados. A integridade garante que as informações permaneçam corretas e não sejam alteradas de maneira não autorizada, protegendo contra adulterações e ataques de manipulação de dados (tampering). Já a disponibilidade visa garantir que os sistemas e os dados estejam acessíveis sempre que necessário, prevenindo falhas ou ataques de negação de serviço (DoS) que possam comprometer seu funcionamento (Whitman *et al.*, 2009). Esses princípios são fundamentais para mitigar riscos e garantir a confiabilidade dos sistemas de informação, especialmente em ambientes críticos, como organizações corporativas e sistemas de saúde.

A segurança como um conceito multifacetado que engloba a proteção dos sistemas de informação contra acessos e ataques não autorizados, garantindo a integridade e a confidencialidade dos dados. Essa perspectiva destaca a necessidade de medidas de segurança robustas em vários ambientes, incluindo ambientes acadêmicos e corporativos. É de suma importância identificar ameaças potenciais e implementar controles para mitigar riscos de forma eficaz aplicando uma abordagem proativa (ANDERSON, 2010).

Segundo Donn B. Parker (2012), as informações são um ativo para as organizações e medidas de segurança devem ser implementadas para protegê-las de uma ampla gama de ameaças. Essa proteção é crucial para manter o valor das informações e a integridade operacional geral da organização. Caso as medidas de segurança não sejam aplicadas, há uma grande chance do comprometimento de informações, observando que as violações podem levar a perdas financeiras significativas, danos à reputação e até repercussões legais para as organizações.

2.3 Engenharia De Requisitos

A Engenharia de Requisitos (ER) desempenha um papel essencial no desenvolvimento de software, identificando, analisando e documentando as necessidades das partes interessadas. Além de atender aos requisitos do usuário, busca alinhar-se aos objetivos do projeto, garantindo eficiência e qualidade. Essa abordagem reduz falhas de comunicação entre stakeholders e desenvolvedores, prevenindo equívocos desde as fases iniciais do projeto (Sommerville, 2011).

É importante criar modelos que representam cenários de trabalho atuais, futuros e hipotéticos. Esses modelos ajudam a visualizar os requisitos e a esclarecer como várias funções contribuem para os objetivos gerais do negócio. O processo de coleta de requisitos é sobre saber quais perguntas fazer para obter uma compreensão abrangente dos stakeholders (Robertson, S; Robertson, J, 2012).

A ER cumpre papel essencial no enfrentamento dos problemas de desenvolvimento de software, trazendo metodologias que permitem estimativa de custo e recursos. Isso é fundamental para gerenciar orçamento e garantir que o projeto permaneça viável financeiramente durante todo o ciclo de vida. O aspecto econômico da engenharia coloca o foco na necessidade de modelos de estimativa de custos confiáveis, uma vez que os custos reais, em geral, superam as estimativas iniciais. Isso demonstra a importância do desenvolvimento de métodos de previsão corretos a fim de minimizar riscos financeiros (Boehm; Barry, 2002).

Diante da relevância desses aspectos, as próximas seções deste trabalho aprofundaram a especificação, modelagem e análise de requisitos, enfatizando sua importância para a segurança e privacidade no desenvolvimento de software. Métodos estruturados de Engenharia de Requisitos possibilitam a identificação e mitigação de riscos, além de garantir conformidade com regulamentações, como a LGPD (Brasil, 2018) e a GDPR (Eu, 2018). A adoção de abordagens sistemáticas voltadas à proteção de dados fortalece a resiliência dos sistemas contra ameaças, assegurando maior controle sobre vulnerabilidades e alinhando-se às melhores práticas do setor (Shostack, 2014).

2.3.1 Especificação de Requisitos

A norma ISO/IEC/IEEE 29148:2018 estabelece orientações para realizar especificações de requisitos, constando que os requisitos devem ser específicos, completos, verificáveis e rastreáveis ao longo do ciclo de vida do sistema. Segundo esta norma, uma boa especificação deve conter requisitos funcionais e não funcionais, devendo especificar também as interfaces e as contradições do sistema; uma boa especificação é aquela que faz os interesses das partes envolvidas serem melhor atendidos. Dessa forma, a adoção destas práticas irá resultar em menor ambiguidade, maior comunicação entre as equipes e menor retrabalho, o que irá ocasionar níveis mais altos da qualidade do software final (ISO/IEC/IEEE, 2018).

Descreve-se que a especificação de requisitos constitui uma fase crítica na engenharia de software, visto que descreve a funcionalidade e as restrições do sistema a ser desenvolvido, de maneira clara e precisa. Uma boa especificação poderá proporcionar uma boa comunicação entre as

partes envolvidas de um projeto e a equipe de desenvolvimento, além de servir de base às atividades subsequentes do projeto (Sommerville, 2011). Constatam Silva et al. (2021) que suficiente clareza e precisão na documentação dos requisitos são essenciais para evitar a ambiguidade e para atender as expectativas dos usuários quanto ao resultado do produto. Uma boa especificação certamente estará associada aos riscos do desenvolvimento e proporcionará um maior alinhamento do software produzido com as necessidades do cliente.

2.3.2 Modelagem de Requisitos

A modelagem de requisitos é um dos processos chave da Engenharia de Software (ES), já que ela possibilita uma melhor compreensão e comunicação sobre as necessidades do sistema entre os stakeholders. A modelagem torna possível organizar e representar graficamente requisitos, facilitando a detecção de incoerências e lacunas. Liebel e Knauss (2023) expressam que, em configurações ágeis de grande porte, a utilização de modelos textuais relacionados aos fluxos de trabalho existentes pode melhorar a rastreabilidade e a evolução dos requisitos através do desenvolvimento.

2.3.3 Análise de Requisitos

A análise de requisitos consiste em examinar e aperfeiçoar os requisitos coletados para garantir que eles possam ser viáveis do ponto de vista técnico e que sejam consistentes com o que é esperado do projeto. Robertson e Robertson (2012) enfatizam que uma análise correta é capaz de revelar requisitos que entram em conflito, classificar prioridades e validar as funcionalidades necessárias para atingir as expectativas dos stakeholders. Ponto em Souza et al. (2019) é que uma análise aprofundada diminui o risco de retrabalho e o repercute no desenvolvimento de sucesso do software. A análise de requisitos ainda abriga técnicas para validar requisitos implícitos, detectar dependências críticas e garantir que todas as partes interessadas compartilhem uma recepção das especificações dadas.

Na ES, a análise de requisitos é um processo crucial, pois permite a avaliação da consistência, viabilidade e completude dos requisitos antes da implementação do sistema. A introdução de abordagens automatizadas se mostra uma alternativa eficiente para minimizar as falhas humanas e acelerar a interpretação dos requisitos coletados.

3. MODELAGEM DE AMEAÇAS E PRIVACIDADE

3.1 Stride

Para auxiliar na identificação e no tratamento estruturado de vulnerabilidades na gestão de riscos, é imprescindível a aplicação de metodologias a fim de levar em consideração as vulnerabilidades dos sistemas de informações, a modelagem de ameaças é uma disciplina central para a realização da integridade, confidencialidade e disponibilidade dos dados. O framework STRIDE, desenvolvido pela Microsoft, é uma ferramenta fundamental nesse processo que fornece um sistema de classificação de ameaças que possibilita a adoção de estratégias eficazes de tratamento das mesmas. Esse modelo tem sido amplamente utilizado em diversas áreas, incluindo o setor de saúde, onde a proteção de informações sensíveis é um requisito crítico.

A aplicação do STRIDE em sistemas de saúde é ainda maior em vista do avanço da digitalização e crescente necessidade da interoperabilidade de diferentes plataformas. A proteção das informações médicas, como os registros eletrônicos de saúde, dados contidos nas informações de saúde e prontuários, têm que ser protegidas contra acessos não autorizados ou uma adulteração indevida e dos vazamentos de informações. Dessa forma, um modelo de segurança capaz de mapear e tratar essas ameaças é fundamental para se assegurar confiabilidade e a conformidade com as regulamentações de proteção de dados.

Além disso, conforme destacado por Franco et al. (2022), a implementação de um planejamento estruturado e orientado para segurança cibernética é essencial para garantir a proteção dos ativos críticos nos sistemas de informação. O estudo propõe um framework para planejamento e gestão de cibersegurança que enfatiza a importância da identificação sistemática de vulnerabilidades e a adoção de controles específicos para mitigação de ameaças.

No contexto da saúde digital, esse tipo de abordagem se mostra indispensável, pois possibilita um planejamento guiado e organizado, considerando tanto os aspectos técnicos quanto os econômicos necessários para uma proteção adequada dos dados sensíveis. A estruturação de medidas preventivas, como autenticação reforçada, monitoramento contínuo e criptografia avançada, fortalece a resiliência dos sistemas contra ameaças classificadas pelo STRIDE, garantindo não apenas a segurança, mas também a continuidade operacional das plataformas de saúde digital.

Segundo Shostack (2014), o STRIDE contribui a compreender possíveis ameaças ao sistema ao dividi-las em seis categorias:

- Spoofing: Ameaças relacionadas com falsificação de identidade.
- Tampering: Modificação não autorizada de dados.
- Repudiation: Ausências de evidências que consigam traçar ações.
- Information Disclosure: Exposição de informações sensíveis.
- Denial of Service (DoS): Tornar os serviços ou sistemas indisponíveis.

Ademais, o STRIDE facilita a identificação de propriedades de segurança específicas que precisam ser mantidas, como autenticação, integridade e confidencialidade, orientando o design de sistemas mais seguros. O modelo pode ser adaptado por meio de variantes como Stride-per-Element, permitindo que as equipes personalizem seu processo de modelagem de ameaças para melhor atender às suas necessidades e contextos específicos, melhorando assim a eficácia de suas medidas de segurança (Kohnfelder; GARG, 1999).

A abordagem da OWASP para modelagem de ameaças, com o STRIDE como elemento chave, promove um processo estruturado e repetitivo que possibilita a identificação proativa de vulnerabilidades, ajudando as organizações a desenvolverem sistemas mais seguros desde as etapas iniciais de seu ciclo de vida.

- **Definir o escopo do trabalho:** Identificar os ativos, pontos de entrada e saída do sistema, além de modelar os fluxos de dados por meio de diagramas (DFDs) para compreender as interações no sistema;
- **Determinar ameaças:** Utiliza o STRIDE como mnemônico para guiar a identificação de ameaças em potencial, permitindo um mapeamento abrangente das vulnerabilidades associadas aos ativos e processos;
- **Mitigar vulnerabilidades:** Identificar contramedidas específicas para cada tipo de ameaça categorizada no STRIDE, como autenticação para mitigar falsificação, uso de hashes e assinaturas digitais para prevenir adulteração, e criptografia para proteger informações confidenciais;

- **Avaliar os resultados:** Validar se as contramedidas implementadas são suficientes para mitigar as ameaças identificadas e revisar iterativamente para melhorar a segurança do sistema.

Levando em conta a situação apresentada por Samavi e Topaloglou (2008), em que Alice busca atendimento em saúde especializada e deve preservar a privacidade dos dados de saúde, implementamos uma modelagem utilizando o framework STRIDE, sendo este um exemplo ilustrativo de quão complexas se tornam as questões de proteção de dados sensíveis em saúde.

Baseando-se no contexto oferecido por Samavi e Topaloglou (2008), o trabalho conseguiu identificar os principais ativos do sistema de informação que diz respeito à gestão dos dados de saúde da Alice, classificado para facilitar a identificação de vulnerabilidades e a aplicação do modelo STRIDE (Tabela 1).

Tabela 1. Ativos do Sistema de Gestão de Dados de Saúde

Nome dos Ativos	**Descrição**
Dados do Paciente	Dados de saúde de Alice, incluindo histórico médico geral, problemas de atenção pré-adolescentes, dados relevantes para tratamentos e desempenho acadêmico.
Registros Eletrônicos de Saúde	Registros compartilhados entre o neurologista, psiquiatra e Instituto de Pesquisa; informações específicas para tratamento e dados sensíveis protegidos.
Controles de Acesso	Políticas que limitam acesso aos dados de Alice apenas ao neurologista, psiquiatra e instituto de pesquisa, com logs e monitoramento de acessos.
Mecanismo de Autenticação	Senhas ou autenticação biométrica para proteger o acesso aos registros médicos de Alice.
Medidas de Segurança	Criptografia dos dados em trânsito e em repouso; protocolos de comunicação seguros para envio ao Instituto de Pesquisa.
Recursos Humanos	Profissionais de saúde (neurologista e psiquiatra) e pesquisadores do Instituto de Pesquisa.
Infraestrutura de Armazenamento	Bancos de dados para armazenar os registros médicos de Alice, tanto a parte privada quanto a parte compartilhável.
Armazenamento na Nuvem	Utilizado pelo instituto de pesquisa para armazenamento temporário dos dados de pesquisa.

3.1.1 Ameaças e vulnerabilidades

1. Spoofing (Falsificação de Identidade):

Ameaças:

- Um atacante pode tentar se passar por neurologista, psiquiatra ou pesquisador do instituto de pesquisa para obter acesso aos dados de saúde de Alice;
- Um atacante pode se disfarçar como usuário legítimo, desse modo, enganado o sistema e tendo acesso às informações confidenciais;
- Falsificação de IP os atacantes podem simular um IP confiável para ter acesso ao sistema; **Vulnerabilidades:**
- Falta de autenticação multifator robusta para profissionais e sistemas;
- Uso de credenciais de acesso fracas ou comprometidas;
- Autenticação de todos os endereços IP e uso de um bloqueador de ataques de rede.

2. Tampering (Alteração de Dados):

Ameaças:

- Modificação não autorizada dos registros de Alice, como histórico médico ou tratamentos, por terceiros;
- Alteração dos dados enviados ao instituto de pesquisa ou entre o neurologista e o psiquiatra.

Vulnerabilidades:

- Dados armazenados ou transmitidos sem criptografia;
- Falta de mecanismos para verificar a integridade dos dados.

3. Repudiation (Negação de Ações):

Ameaças:

- O Instituto de Pesquisa alega que não recebeu os dados de Alice, mesmo após o envio por parte do psiquiatra;
- O instituto de pesquisa pode negar a exclusão dos dados após o fechamento do caso;

- O neurologista percebe que os registros de Alice foram alterados, mas nenhum dos profissionais admite a modificação.

Vulnerabilidades:

- Falta de trilhas de auditoria (logs) confiáveis para monitorar acessos e modificações nos registros;
- Ausência de *timestamps* ou assinaturas digitais em transações críticas;
- Ausência de mecanismos de rastreio ou controle de integridade dos registros.

4. Information Disclosure (Divulgação de Informações):

Ameaças:

- Vazamento de dados sensíveis, como o problema de atenção de Alice, para partes não autorizadas;
- Interceptação de dados durante a transmissão ao instituto de pesquisa.

Vulnerabilidades:

- Comunicação sem uso de protocolos seguros como TLS;
- Controle de acesso inadequado permitindo acesso indevido a informações sensíveis.

5. Denial of Service (Negação de Serviço):

Ameaças:

- Interrupção do sistema de registros de saúde ou do acesso do neurologista, ou psiquiatra aos dados de Alice;
- Ataque ao instituto de pesquisa, tornando-o incapaz de processar os dados de Alice durante a análise.

Vulnerabilidades:

- Falta de proteção contra picos de tráfego ou recursos limitados no sistema; ● Dependência de um único ponto de falha para acesso aos dados.

6. Elevation of Privilege (Elevação de Privilégio):

Ameaças:

- Um atacante pode explorar vulnerabilidades no sistema para obter privilégios administrativos, permitindo acesso total aos dados de Alice;
- Um pesquisador do instituto de pesquisa pode tentar acessar dados não relacionados ao caso de Alice.

Vulnerabilidades:

- Configurações inadequadas de controle de acesso;
- Privilégios excessivos concedidos a usuários ou sistemas.

A crescente digitalização no setor da saúde trouxe avanços significativos, incluindo a interoperabilidade entre sistemas e uma troca eficiente de informações médicas entre profissionais e instituições. Contudo, essa transformação também intensificou os riscos relacionados à privacidade e à segurança dos dados dos pacientes. O sistema de saúde contemporâneo é formado por uma rede de diversos atores, como pacientes, médicos, instituições de pesquisa e plataformas de armazenamento de dados, todos sujeitos a regulamentações de proteção, incluindo a GDPR e a LGPD.

No cenário da paciente Alice, que se encontra na tese de Peixoto (2021), o sistema de saúde é projetado para permitir um compartilhamento de informações médicas que é tanto seletivo quanto controlado. Alice, uma paciente em busca de atendimento especializado, deseja manter a confidencialidade de partes de seu histórico médico ao se consultar com um neurologista e um psiquiatra. Ademais, a interação desses médicos com um instituto de pesquisa focado no TDAH (Transtorno de Déficit de Atenção e Hiperatividade) adiciona um nível adicional de complexidade ao fluxo de dados, exigindo a implementação de mecanismos robustos para autenticação, controle de acesso e auditoria.

Nesse cenário, a segurança das informações médicas se torna um aspecto fundamental do sistema de saúde. É imprescindível identificar e mitigar ameaças que possam prejudicar a integridade, a confidencialidade e a disponibilidade dos dados. Em conformidade com o método descrito por Ilg et al. (2023), o modelo STRIDE foi utilizado para identificar ameaças aos ativos do sistema de saúde, categorizando os tipos de ataque de acordo com os ativos e suas consequências.

Assim, como no caso dos veículos definidos por software, a aplicação do STRIDE estabelece uma ligação direta entre ativos críticos, como os dados dos pacientes, e ameaças como

spoofing (falsificação de identidade) e information disclosure (exposição de informações), auxiliando na definição e na implementação dos controles de segurança adequados.

Em consonância com o método descrito por Ilg (et al., 2023), o modelo STRIDE foi adotado para detectar ameaças visando os ativos do sistema de saúde, categorizando os tipos de ataque em relação aos ativos e ao impacto destes. Tal como no caso dos veículos definidos por software, a aplicação do STRIDE cria uma correlação direta entre ativos críticos, ajudando na adequação dos controles de segurança necessários (Tabela 2).

Tabela 2. Análise de Ameaças e Vulnerabilidades no Sistema de Saúde utilizando o Modelo STRIDE

Tipos de Elementos	S	T	R	I	D	E
Paciente (Alice)	X			X		
Profissionais de Saúde	X		X			X
Registros Eletrônicos de Saúde	X	X	X	X	X	
Fluxo de Dados		X		X	X	
Armazenamento em Nuvem		X		X		X

Tipos de Elementos:

- **Paciente (Alice)**: É um ator externo que fornece os dados, sendo suscetível a falsificação de identidade (Spoofing) e à violação de confidencialidade (Information Disclosure).
- **Profissionais de Saúde**: Incluem neurologistas, psiquiatras e pesquisadores que interagem com os dados. Podem ser alvos de falsificação (Spoofing), negação de ações (Repudiation) e elevação de privilégios (Elevation of Privilege).
- **Registros Eletrônicos de Saúde**: São o repositório principal de dados e podem ser afetados por falsificação (Spoofing), alteração (Tampering), negação de ações (Repudiation), violação

de confidencialidade (Information Disclosure) e ataques de negação de serviço (Denial of Service).

- **Fluxo de Dados**: Envolve a transmissão de informações, podendo ser afetado por alterações (Tampering), violação de confidencialidade (Information Disclosure) e interrupções (Denial of Service).
- **Armazenamento em Nuvem**: Usado para armazenamento temporário, pode sofrer alterações (Tampering), violações de confidencialidade (Information Disclosure) e elevação de privilégios (Elevation of Privilege).

3.1.2 Técnicas de mitigação e ameaças STRIDE

No contexto da análise de segurança empregando o modelo STRIDE, é imprescindível considerar as abordagens de mitigação específicas para cada ameaça apresentada. A respeito das ameaças, a OWASP Foundation classifica diferentes categorias, tais como, falsificação da identidade, adulteração de dados, repúdio, revelação de informações, negação de serviços e elevação de privilégio, para as quais técnicas de mitigação recomendadas são utilizadas com a finalidade de minimizar os riscos e proteger os bens de um sistema. A Tabela a seguir apresenta a relação entre as estratégias de mitigação para cada tipo de ameaça STRIDE, tal como descrito no relatório de modelagem de ameaças da OWASP (2025) (Tabela 3).

Tabela 3. Ameaças e Mitigações STRIDE

Tipo de ameaça	Técnicas de mitigação
Falsificação de identidade	1. Autenticação apropriada 2. Projeta dados secretos 3. Não armazena segredos
Adulteração de dados	1. Autorização apropriada 2. Hashes 3. MACs 4. Assinaturas digitais 5. Protocolos resistentes a adulteração
Repúdio	1. Assinaturas digitais 2. Carimbos de data e hora 3. Trilhas de auditoria
Divulgação de informações	1. Autorização 2. Protocolos de privacidade aprimorada 3. Criptografia 4. Projeta segredos 5. Não armazena segredos
Negação de serviço	1. Autenticação apropriada 2. Autorização apropriada 3. Filtragem 4. Limitação 5. Qualidade do serviço
Elevação de privilégio	1. Execute com o mínimo de privilégios

3.2 LINDDUN

O LINDDUN é caracterizado como uma estrutura integrada de modelagem de ameaças, restrita a ameaças à privacidade, que apresenta suporte e know-how dos processos de identificação de ameaças no âmbito da privacidade com relação ao desenvolvimento de sistemas de software. Ela é integrada aos ciclos de vida de desenvolvimento de software seguro (SDLC), com o enfoque em descobrir falhas de design relacionadas à privacidade em um estágio inicial do conceito de arquitetura (Van Landyt; Joosen, 2020).

Além disso, ele oferece uma modelagem de ameaças, que faz o agrupamento de em categorias específicas relacionadas à privacidade, desse modo, ajuda as equipes a lidar sistematicamente com as possíveis ameaças. A usabilidade do LINDDUN é favorecida por sua capacidade de facilitar a comunicação entre os membros da equipe, pois fornece uma linguagem que seja acessível a todos, mesmo para aqueles que não tenham muita experiência no domínio de segurança. O alcance da estrutura vai além da modelagem de ameaças, ela também oferece suporte para a priorização destas últimas, a partir do efeito que elas possuem, permitindo que as equipes se concentrem primeiramente nas questões mais problemáticas (Deng, Mina et al., 2011).

O processo de análise de ameaças toma como partida a instalação do Diagrama de Fluxo de Dados (DFD), que representa a arquitetura do sistema e o fluxo de dados que opera ao longo do tempo. Aperfeiçoando esse diagrama, mediante a estrutura LINDDUN, as ameaças à privacidade são sistematicamente visíveis, sendo classificada em vinculabilidade, identificabilidade, não repúdio, detectabilidade, divulgação de informações, desconhecimento e não conformidade. As ameaças levantadas recebem propostas de mitigação que se convertam em medidas para reforçar a privacidade do sistema, garantindo sua proteção contra os riscos encontrados (Nweke, et al., 2022).

3.2.1 Diagrama de Fluxo de dados

O Diagrama de Fluxo de Dados (DFD) desenvolvido para o cenário da paciente Alice respeita os princípios estabelecidos por Nweke et al. (2022, p. 5). Este diagrama representa a interação das entidades participantes (paciente, neurologista, psiquiatra e instituição de pesquisa), o sistema de gerenciamento de dados e os fluxos de dados para o atendimento e análise das informações de saúde de Alice.

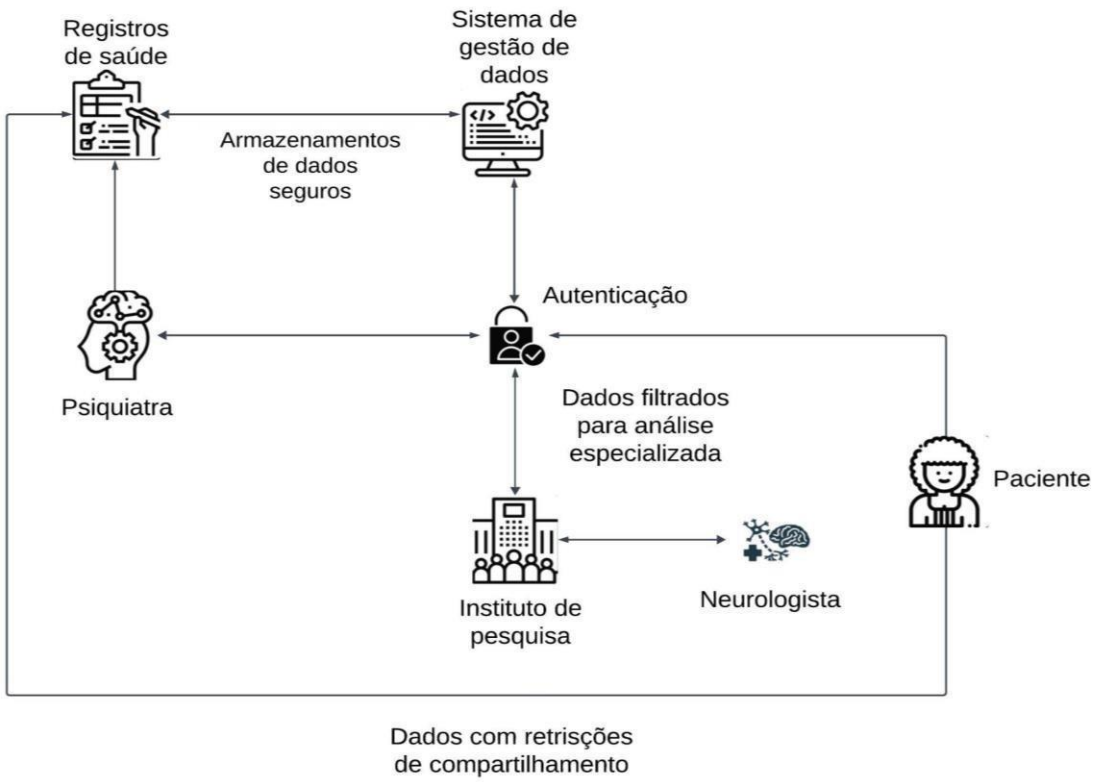
Para garantir a completude do mapeamento de ameaças no DFD, foi realizada uma análise detalhada baseada no modelo de Nweke et al. (2022). Essa revisão identificou a necessidade de incluir fluxos de dados internos (como a comunicação entre médicos e o instituto de pesquisa), interação do usuário com o sistema (permitindo que Alice gerencie suas permissões) e mecanismos de

armazenamento temporário (se houver retenção de logs no instituto de pesquisa). Essas inclusões permitem um mapeamento mais preciso das ameaças e reforçam a aderência do estudo às melhores práticas de modelagem de ameaças à privacidade.

A Figura 1 descreve DFD que ilustra o processo de compartilhamento e análise de dados de saúde no cenário da paciente Alice. A figura mostra a interação entre as diferentes entidades envolvidas, como o paciente (Alice), o psiquiatra, o neurologista e o instituto de pesquisa. O fluxo de dados é controlado por um sistema de gerenciamento de dados seguro, que garante que apenas informações relevantes sejam compartilhadas, respeitando as permissões de Alice.

Além disso, a autenticação é destacada, assegurando que os dados sejam acessados apenas por entidades autorizadas. A figura enfatiza os dados com restrições de compartilhamento, ou seja, aqueles que Alice não deseja divulgar, como o histórico relacionado ao transtorno de déficit de atenção. A visualização facilita a compreensão de como as informações são processadas e acessadas dentro do sistema, oferecendo uma visão clara dos fluxos e das interações críticas no tratamento e análise dos dados de saúde.

Figura 1. Diagrama de Fluxo de dados



3.2.2 Mapeamento de Ameaças à privacidade com base no modelo de mapeamento LINDDUN

O mapeamento de ameaças à privacidade no cenário da paciente Alice foi estruturado com base no modelo LINDDUN, conforme apresentado por Nweke et al. (2022, p. 5). Este modelo permitiu identificar ameaças específicas relacionadas às categorias de privacidade, incluindo Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness e Noncompliance. No caso de Alice, os riscos mapeados incluem a possibilidade de vinculação de seus dados médicos com outras informações, identificação indevida por meio de dados sensíveis transmitidos, bem como falhas na exclusão de informações pelo instituto de pesquisa após o uso. Cada elemento do sistema como as entidades (Alice, neurologista, psiquiatra, instituto de pesquisa), os processos (gestão de dados, autenticação), os armazenamentos (registros médicos) e os fluxos de dados — foi analisado para identificar ameaças potenciais que poderiam comprometer a privacidade de Alice durante o compartilhamento e uso de seus dados de saúde (Tabelas 4, 5, 6, 7).

Tabela 4. Entidades

Entidade	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Alice	X	X			X	X	
Neurologista		X	X			X	
Psiquiatra		X	X			X	
Instituto de Pesquisa	X	X		X	X		X

Tabela 5. Processos

Processos	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Sistemas de gestão de dados	X	X		X	X		X
Autenticação		X	X			X	

Tabela 6. Armazenamento de Dados

Armazenamento	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Registros de saúde	X	X			X		X

Tabela 7. Fluxo de Dados

Fluxo de dados	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Dados com restrições de compartilhamento	X	X			X		X
Dados filtrados para análise	X	X			X		X

3.2.3 Explicação das Ameaças:

1. **Linkability (L):**
    - **Risco:** Os dados de saúde de Alice podem ser vinculados a outras informações pessoais, revelando informações sensíveis.
2. **Identifiability (I):**
    - **Risco:** Identificação direta de Alice com base nos dados transmitidos, como biometria ou histórico.
3. **Non-repudiation (N):**
    - **Risco:** Médicos ou pesquisadores podem negar acessos ou alterações nos dados.
4. **Detectability (D):**
    - **Risco:** Detectar que Alice é usuária do sistema, mesmo sem acessar seus dados.
5. **Disclosure of Information (D):**
    - **Risco:** Vazamento de informações confidenciais durante a transmissão ou armazenamento.
6. **Unawareness (U):**
    - **Risco:** Alice não sabe como seus dados estão sendo usados ou compartilhados.
7. **Non-compliance (N):**
    - **Risco:** O Instituto de Pesquisa não exclui os dados conforme solicitado.

3.2.4 Suposições das Ameaças no Cenário da Paciente Alice

No cenário da paciente Alice foram identificadas e categorizadas ameaças à privacidade segundo o método LINDDUN, seguindo a linha de raciocínio utilizada por Nweke et al. (2022, p. 5). As ameaças foram classificadas em relação aos níveis de riscos que as ameaças representam para a privacidade da paciente no fluxograma dos dados. Em seguida, são elencadas as principais suposições para cada categoria de ameaça.

1) **Linkability (Vinculação de dados) Suposição**: O sistema pode permitir que os dados de Alice sejam vinculados por meio de consultas, de modo a poder inferir informações confidenciais sobre ela, mesmo que não haja acesso aos seus registros médicos;

   I. **Impacto**: Alto - Pode permitir que terceiros, como o Instituto de Pesquisa, relacionem dados históricos de Alice com novas consultas, violando suas preferências de compartilhamento.

2) **Identifiability (Identificação) Suposição**: Os dados médicos de Alice , mesmo podendo ser parcialmente compartilhados , podem conter dados suficientes para a identificação única da paciente, como histórico de doenças raras ou exames específicos;
   I. **Impacto**: Alto - A exposição de dados identificáveis pode comprometer o anonimato da paciente e permitir que seus dados sejam rastreados indevidamente.
3) **Non-repudiation (Não repúdio) Suposição**: O Instituto de Pesquisa pode alegar que não recebeu ou processou os dados de Alice, dificultando auditorias e a exigência de conformidade;
   I. **Impacto**: Médio - A falta de mecanismos de auditoria pode obstruir Alice na prova de a quem seus dados foram dados e como eles foram utilizados e de que maneira foram eliminados.
4) **Detectability (Detectabilidade) Suposição**: Mesmo sem acesso direto aos registros médicos, pode-se identificar Alice como a paciente do neurologista e do psiquiatra, a partir do volume de acessos que estão registrados no sistema de gestão de dados;
   I. **Impacto**: Médio - A exposição da frequência do uso do sistema pode permitir inferir que Alice é tratada para certas condições médicas.
5) **Disclosure of Information (Divulgação de Informações) Suposição**: Os dados de saúde de Alice podem ser vazados para partes não autorizadas durante a transmissão entre o sistema de gestão de dados e o Instituto de Pesquisa;
   I. **Impacto**: Alto – A exposição de informações médicas pode comprometer a privacidade da paciente e levá-la a consequências indesejadas, como discriminação.
6) **Unawareness (Desconhecimento) Suposição**: Alice pode não estar totalmente ciente de como seus dados estão sendo processados e compartilhados, especialmente em relação ao armazenamento no Instituto de Pesquisa;
   I. **Impacto**: Alto – A falta de clareza sobre o uso de seus dados pode levar a consentimentos inadequados e à exposição de informações que Alice não deseja compartilhar.
7) **Non-compliance (Não Conformidade) Suposição**: O Instituto de Pesquisa pode falhar em excluir os dados de Alice conforme prometido, mantendo informações armazenadas além do necessário;

I. **Impacto**: Alto – O não cumprimento dos requisitos de exclusão compromete a privacidade e os direitos da paciente sobre seus próprios dados.

A tabela a seguir se baseia na estrutura das Tabelas II e III do artigo de Nweke et al. (2022, p. 5). (2017), adaptando-as para o cenário da paciente Alice. Cada elemento do DFD é avaliado em relação às ameaças LINDDUN (Tabela 8).

Tabela 8 – Mapeamento de Ameaças à Privacidade no Cenário da Paciente Alice

Elemento do DFD	**L**	**I**	**N**	**D**	**D**	**U**	**N**
Paciente (Alice)	X	X			X	X	
Neurologista		X	X			X	
Psiquiatra		X	X			X	
Instituto de Pesquisa	X	X		X	X		X
Sistema de Gestão de Dados	X	X		X	X		X
Autenticação		X	X			X	
Registros de Saúde	X	X			X		X

Tabela 9 – Estratégias de Mitigação das Ameaças à Privacidade

Threat (Ameaça)	**Mitigation Strategy (Estratégia de Mitigação)**	**Privacy Requirement (Requisito de Privacidade)**	**Suggested Privacy Enhancing Solution (Solução Reforçada de Privacidade)**
Identificação de Alice a partir de seus dados de saúde	Anonimização, Confidencialidad, Pseudonimização	Garantir que Alice não possa ser identificada a partir de seus dados biomédicos ou históricos médicos	Aplicar técnicas de anonimização como k-anonymity, proteger os dados com controle de acesso baseado em papéis (RBAC) e utilizar pseudonimização de identificadores
Divulgação de informações sensíveis de Alice	Confidencialidade	Garantir a proteção dos dados de Alice nos registros médicos e no Instituto de Pesquisa	Aplicar controle de acesso baseado em papéis nos bancos de dados médicos e usar criptografia ISO para proteção de registros
Falsificação de credenciais para acessar os dados de Alice	Autenticação	Garantir que apenas usuários autorizados possam acessar os dados médicos	Implementar autenticação multifator (MFA) para médicos e pesquisadores
Interceptação dos dados médicos durante a transmissão	Confidencialidade	Garantir que os dados não sejam acessados por terceiros durante a comunicação entre os sistemas	Usar criptografia TLS para proteger a comunicação entre o sistema de gestão de dados e o Instituto de Pesquisa
Exposição indevida dos dados no Instituto de Pesquisa	Confidencialidade	Garantir que os dados de Alice sejam armazenados e excluídos	Implementar logs de auditoria e aplicar políticas de retenção e exclusão de dados conforme definido por Alice

		corretamente após sua utilização	
Falta de transparência no uso dos dados de Alice	Conscientização	Garantir que Alice compreenda como seus dados estão sendo utilizados	Implementar um painel de controle para que Alice visualize e gerencie suas preferências de compartilhamento
Persistência dos dados de Alice no Instituto de Pesquisa após o encerramento do caso	Conformidade	Garantir que os dados sejam excluídos após o uso, conforme as diretrizes de privacidade estabelecidas	Implementar auditorias regulares e contratos inteligentes que garantam a exclusão automática dos dados após o término da pesquisa

A tabela 9 adapta as estratégias de mitigação do artigo de Nweke et al. (2022, p. 5) ao cenário da paciente Alice, garantindo que as ameaças identificadas no mapeamento LINDDUN sejam tratadas de forma eficaz. As soluções propostas incluem anonimização, pseudonimização, criptografia robusta, autenticação multifator e auditorias regulares para garantir que os dados de Alice sejam protegidos contra acessos indevidos e permaneçam sob seu controle.

3.3 Privacy Criteria Method

São necessárias abordagens sistemáticas para especificar requisitos de privacidade e o PCM surge justamente para orientar desenvolvedores de software na especificação de requisitos de privacidade no desenvolvimento, visando ajudar os desenvolvedores no processo de controle de privacidade desde os estágios iniciais (Peixoto e Silva, 2018).

O PCM é resultado de um *Framework* de Capacidades de Especificação de Privacidade. O *framework* contém 12 capacidades, que são:

1. Especificação do objetivo do contexto das tarefas;
2. Especificação de diferentes tipos de atores;
3. Especificação de relacionamentos entre atores;
4. Especificação da relação de confiança;
5. Especificação dos diferentes tipos de informações pessoais;
6. Especificação dos mecanismos de privacidade;
7. Especificação da restrição de privacidade (preferência de privacidade ou conformidade de privacidade/política);
8. Especificação dos riscos de privacidade;
9. Especificação das ameaças de privacidade;
10. Especificação dos danos à privacidade;
11. Especificação da vulnerabilidade de privacidade;
12. Especificação do cenário de risco - Capacidade de conectar riscos, ameaças, danos e vulnerabilidade.

Segundo Peixoto e Silva (2021), O PCM possui um identificador (ID) e uma descrição do requisito. Ele é definido por um requisito de privacidade e pode ter um dos quatro tipos de prioridade: Baixo Crítico; Regular; Crítico; e Muito Crítico. Cada Requisito de Privacidade tem pelo menos um Stakeholder.

As informações pessoais são protegidas pelo Mecanismo de Privacidade e podem estar relacionadas com zero ou mais Restrições de Privacidade. É restrito por um Contexto de Propósito e tem pelo menos um Proprietário/Controlador. Proprietário/Controlador, Processador e Terceiros se relacionam entre si.

O PCM tem pelo menos uma informação pessoal que pode ser: pública, privada ou semipública. O PCM pode ter zero ou mais restrições de privacidade que podem ser: Preferência de Privacidade e/ou Conformidade/Política de Privacidade. O PCM pode ter um ou mais cenários de risco que, por sua vez, têm pelo menos um dano. Uma vulnerabilidade é explorada por uma ameaça, resultando em danos ao sistema. Finalmente, o PCM tem pelo menos um mecanismo de privacidade para atenuar um cenário de risco.

O exemplo ilustrativo apresentado neste trabalho baseia-se no cenário da paciente Alice, descrito na tese de Peixoto (2021). O caso explora as complexidades do compartilhamento seletivo de informações médicas em um ambiente de saúde conectado, no qual Alice deseja preservar a confidencialidade de partes do seu histórico médico ao consultar um neurologista e um psiquiatra. Além disso, a interação desses profissionais com um instituto de pesquisa focado no Transtorno do Déficit de Atenção e Hiperatividade (TDAH) adiciona desafios à privacidade e segurança dos dados. Para analisar esse cenário, será realizada uma avaliação detalhada das ameaças à segurança e privacidade que surgem nesse contexto, utilizando a modelagem STRIDE para identificar estratégias de mitigação de riscos à segurança e LINDDUN para levantar ameaças à privacidade.

Com base nessa análise, foram criados artefatos para representar os requisitos de privacidade e segurança necessários à proteção dos dados de Alice. Esses artefatos foram desenvolvidos a partir da integração do Privacy Criteria Method (PCM) com os métodos STRIDE e LINDDUN, permitindo um mapeamento mais preciso das ameaças e a proposição de estratégias de mitigação. O objetivo desta seção é demonstrar como a abordagem integrada pode auxiliar na especificação e tratamento de riscos, garantindo um modelo mais seguro e alinhado às necessidades dos usuários e aos regulamentos de privacidade.

Embasado nesse cenário retirado da documentação do PCM, foram criados os seguintes artefatos:

- **USER STORIES**: Como usuário de assistência médica, quero ter registro para poder acessar o sistema.
- **CRITÉRIO DE ACEITAÇÃO**:
  1. O registro deve conter nome de usuário *, e-mail * e senha *;
  2. O nome de usuário deve ser exclusivo;
  3. A senha deve conter números, letras e caracteres;
  4. Para salvar, é necessário que todos os campos obrigatórios (*) sejam preenchidos;
  5. O código sequencial para identificar o registro deve ser gerado pelo banco de dados.

A estrutura do Privacy Criteria Method (PCM) é composta por elementos essenciais que orientam a especificação de requisitos de privacidade em sistemas de software. A modelagem começa pela identificação dos atores (Actors), ou seja, os indivíduos, organizações ou sistemas envolvidos no processamento de informações pessoais. Esses atores podem incluir usuários finais, prestadores de

serviço, terceiros e reguladores, sendo fundamental compreender seus papéis e responsabilidades no fluxo de dados.

No cenário da paciente Alice, os principais atores envolvidos são Alice (paciente), o neurologista, o psiquiatra e o Instituto de Pesquisa, com cada um deles tendo um papel distinto no acesso e no uso das informações de saúde de Alice. Por exemplo, Alice é quem fornece os dados e utiliza os serviços de saúde, enquanto o neurologista e o psiquiatra são os profissionais responsáveis pelo gerenciamento e acesso desses dados. O Instituto de Pesquisa, por sua vez, pode processar as informações para fins científicos, desde que haja o devido consentimento por parte de Alice.

A segunda etapa aborda as relações de confiança entre os atores (Actors' Trust Relationship (Disclosure), que determinam como as informações são compartilhadas entre diferentes entidades. Esse relacionamento define quais atores podem acessar determinados dados e sob quaisquer circunstâncias, garantindo que a transparência e a conformidade regulatória sejam mantidas.

No caso de Alice, essa etapa envolve definir os termos sob os quais suas informações serão compartilhadas. Alice confia que seus dados serão compartilhados de maneira restrita e com base no seu consentimento. Ela deseja compartilhar seus dados médicos apenas com o psiquiatra, mas não com o neurologista, e espera que o Instituto de Pesquisa utilize suas informações de forma controlada e exclusivamente para os fins de seu tratamento.

A identificação e classificação dos tipos de dados pessoais tratados são fundamentais no PCM. No caso de Alice, os dados pessoais envolvem seu nome, histórico médico, diagnósticos e informações sobre transtornos psicológicos, como o transtorno de déficit de atenção que ela deseja manter em sigilo. Esses dados precisam ser protegidos contra acessos indevidos, com controles claros sobre quem tem permissão para acessá-los e para quais finalidades.

A estrutura do PCM também define o propósito do contexto da tarefa (The Purpose of Task Context {Use/Retention}), estabelecendo por que os dados estão sendo coletados, como serão utilizados e por quanto tempo serão retidos. Essa definição é fundamental para evitar o armazenamento excessivo de informações e garantir que a retenção de dados esteja alinhada com as diretrizes de Privacy by Design e conformidade regulatória, como a LGPD e a GDPR.

A estrutura do PCM define o propósito do contexto da tarefa (The Purpose of Task Context {Use/Retention}), estabelecendo por que os dados estão sendo coletados, como serão utilizados e por quanto tempo serão retidos. Essa definição é fundamental para evitar o armazenamento excessivo de informações e garantir que a retenção de dados esteja alinhada com as diretrizes de Privacy by Design e conformidade regulatória, como a LGPD e a GDPR.

No caso de Alice, seus dados serão utilizados para diagnóstico e tratamento. Ela concorda em compartilhá-los com o psiquiatra, mas somente para fins de tratamento e enquanto o caso estiver ativo. Alice também espera que seus dados sejam excluídos do sistema de forma definitiva quando não forem mais necessários.

Outro componente essencial do PCM são as restrições de privacidade (Privacy Constraints), que representam limitações impostas ao processamento de dados pessoais. Essas restrições podem incluir consentimento do usuário, regras de anonimização, requisitos legais ou políticas organizacionais que precisam ser seguidas para garantir que os dados sejam tratados de forma ética e segura.

Aqui, são definidas as restrições e obrigações impostas ao processamento dos dados pessoais. No caso de Alice, ela impõe restrições específicas quanto ao compartilhamento de seus dados. Por exemplo, ela deseja que suas informações sejam acessadas apenas para fins de tratamento médico, não permitindo o uso para outros objetivos, como pesquisa, sem seu consentimento explícito.

Com base nas informações coletadas, o PCM permite a modelagem de cenários de risco (Privacy Risk Scenario), onde são identificadas possíveis ameaças à privacidade, como acessos não autorizados, vazamento de informações e processamento indevido de dados. Cada cenário de risco descreve o impacto da ameaça, os atores envolvidos e as potenciais consequências para os usuários, permitindo uma visão clara dos riscos associados ao sistema.

No caso de Alice, o PCM permite identificar cenários de risco como a possibilidade de seu transtorno de déficit de atenção ser exposto sem seu consentimento, ou o risco de um profissional de saúde acessar dados além do necessário para o tratamento. Esses cenários destacam as ameaças específicas enfrentadas por Alice, ajudando a entender as potenciais consequências para sua privacidade e a importância de implementar medidas adequadas para mitigação desses riscos.

Por fim, a estrutura do PCM inclui a definição de mecanismos de privacidade (Privacy Mechanisms), que correspondem às medidas técnicas e organizacionais implementadas para mitigar os riscos identificados. Esses mecanismos podem incluir criptografia, autenticação multifator, pseudonimização, políticas de acesso restrito e anonimização de dados. A adoção desses mecanismos garante que as ameaças identificadas nos cenários de risco sejam reduzidas e que os requisitos de privacidade sejam atendidos de maneira eficaz.

No caso de Alice, isso pode envolver criptografia de dados, autenticação multifatorial e controles de acesso restritos, garantindo que apenas os profissionais autorizados possam acessar as informações de Alice, conforme as restrições acordadas. Esses mecanismos são fundamentais para

proteger seus dados contra acessos não autorizados e garantir que as informações sensíveis sejam tratadas de maneira segura e em conformidade com as exigências regulatórias.

Dessa forma, a estrutura do PCM fornece um modelo estruturado para a identificação, análise e mitigação de riscos à privacidade, ajudando desenvolvedores e engenheiros de requisitos a projetar sistemas mais seguros e transparentes. Ao conectar atores, informações, restrições e mecanismos de proteção, o PCM possibilita uma abordagem integrada e eficaz para a Engenharia de Requisitos.

Por meio do USER STORY e dos CRITÉRIOS DE ACEITAÇÃO, foi possível a criação do Privacy Criteria Artifact (Figura 2).

Figura 2 - Estrutura do PCM

<table>
<tr><td>ID (PC01)</td><td colspan="2">Privacy Requirement: Health Care User Registration</td><td>Source: Alice
Priority: Critical</td></tr>
<tr><td colspan="3">Description: The system should allow the inclusion of new users.</td><td>2 - Actors' Trust Relationship (disclosure)</td></tr>
<tr><td rowspan="3">1 - Actors</td><td>Owner/Controller</td><td>Health Care User</td><td>System</td></tr>
<tr><td>Processor</td><td>System</td><td></td></tr>
<tr><td>Third Party</td><td></td><td></td></tr>
<tr><td colspan="3"></td><td>4 - The purpose of task context (use/retention)</td></tr>
<tr><td rowspan="3">3- Personal Information

(collect)</td><td>Private</td><td>Password, Email, UserName, IdPerson</td><td>For system registration</td></tr>
<tr><td>Public</td><td></td><td></td></tr>
<tr><td>Semi-Public</td><td></td><td></td></tr>
<tr><td>5 - Privacy Constraint:</td><td>Privacy Preference</td><td colspan="2"></td></tr>
</table>

<table>
<tr><td></td><td>Privacy Compliance/Policy</td><td colspan="2">- Other users may not be able to view data marked as private.</td></tr>
<tr><td rowspan="2">6 - Privacy Risk Scenario</td><td>Potential Vulnerability</td><td rowspan="2">EXPLORED BY</td><td>Potential Threat</td></tr>
<tr><td>- Other user can access user’s Password, UserName,</td><td>Exposure of user's registration</td></tr>
<tr><td rowspan="4"></td><td>IdPerson and email</td><td></td><td></td></tr>
<tr><td colspan="3">CAUSE</td></tr>
<tr><td colspan="3">Potential Harm</td></tr>
<tr><td colspan="3">Unrestricted access to all user information</td></tr>
<tr><td>7 - Privacy Mechanisms</td><td colspan="3">● Access control with notification via health care user email.</td></tr>
</table>

Fonte: Peixoto, 2021. (Privacy Requirement – 01)

3.3.1 Definição do Contexto e Atores

A proposta deste trabalho será ilustrada no contexto de um sistema de saúde, no qual a privacidade dos dados médicos dos pacientes deve ser garantida por meio de mecanismos estruturados de proteção e controle de acesso. Para isso, será utilizado o caso de uma paciente chamada Alice, descrito na tese de Peixoto (2021), que apresenta um cenário no qual a paciente deseja manter a confidencialidade de partes do seu histórico médico ao interagir com diferentes profissionais da área da saúde.

Nesse contexto, Alice consulta um neurologista devido a dores nos pulsos, mas prefere não compartilhar seu histórico de transtorno de déficit de atenção ocorrido na pré-adolescência. Entretanto, essa mesma informação será discutida posteriormente com um psiquiatra, que avaliará seu desempenho acadêmico recente. Adicionalmente, os dados de Alice podem ser compartilhados com um instituto de pesquisa especializado em TDAH, exigindo a implementação de mecanismos que garantam a restrição de acesso e o uso controlado dessas informações.

O sistema de saúde utilizado por Alice deve, portanto, assegurar que seus dados sejam compartilhados apenas com os atores autorizados e para finalidades previamente definidas, garantindo que as informações não sejam expostas indevidamente ou armazenadas além do necessário. Mais detalhes sobre esse cenário podem ser encontrados na Seção 3.3, onde o caso de Alice é apresentado de forma estruturada e aprofundada.

- **Paciente**: Pessoa que fornece os dados e utiliza os serviços de saúde;
- **Médico (Neurologista e Psiquiatra)**: Profissionais que acessam e gerenciam os dados;
- **Instituto de Pesquisa**: Entidade que pode processar informações para fins científicos;
- **Sistema de Gestão de Dados**: Plataforma que centraliza e armazena os dados médicos;
- **Banco de Dados de Registros de Saúde**: Repositório onde os dados médicos são armazenados.

3.3.2 Classificação dos Dados no PCM

1. **Atores (Actors)**: Representam as entidades envolvidas no processamento das informações pessoais. Isso pode incluir usuários, sistemas, prestadores de serviços e reguladores;
    I. No caso de Alice: Os principais atores envolvidos incluem Alice (paciente), o neurologista, o psiquiatra e o Instituto de Pesquisa. Cada um desses atores tem um papel distinto no acesso e no uso de suas informações de saúde.
2. **Relação de Confiança dos Atores (Actors' Trust Relationship - Disclosure)**: Define os relacionamentos de confiança entre os atores, estabelecendo quais informações podem ser compartilhadas e sob quais condições;
    I. No caso de Alice: Alice confia que seus dados serão compartilhados de forma restrita e conforme sua permissão. Por exemplo, ela deseja compartilhar seu histórico médico com seu psiquiatra, mas não com o neurologista. Além disso, ela espera que o Instituto de Pesquisa trate seus dados de forma segura.
3. **Informação Pessoal (Personal Information)**: No contexto da proteção de dados e privacidade, as informações pessoais podem ser classificadas em três categorias principais: público, privado e semipúblico. Cada uma dessas categorias possui características próprias que determinam o nível de acesso, compartilhamento e segurança exigidos;
    I. **Dados Públicos**: Refere-se àquelas informações pessoais que são acessíveis ao público em geral, seja por serem divulgadas pelo próprio indivíduo ou por estarem disponíveis

por meio de fontes públicas. Exemplos típicos incluem o nome completo, endereço de e-mail profissional, cargo ocupacional e outras informações que o indivíduo opta por compartilhar publicamente. Esses dados podem ser acessados sem restrição, mas sua coleta e uso ainda devem respeitar as leis de privacidade e consentimento, especialmente no caso de seu uso para fins comerciais;

II. **Dados Privados**: São informações pessoais sensíveis, que dizem respeito a aspectos íntimos da vida de um indivíduo, e que não devem ser acessadas ou compartilhadas sem o consentimento explícito da pessoa envolvida. No contexto de saúde, por exemplo, esses dados incluem histórico médico, diagnósticos, exames e outros registros que estão protegidos por regulamentações rigorosas, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. A coleta, armazenamento e uso desses dados devem ser realizados com controle estrito e garantias de que o acesso será limitado aos profissionais autorizados;

III. **Dados Semipúblicos**: São aqueles dados que, embora possam ser acessados por certos grupos ou sob determinadas condições, não são completamente públicos e estão sujeitos a restrições. Isso pode incluir, por exemplo, informações que podem ser visualizadas por uma rede restrita, como membros de uma organização ou profissionais de um determinado setor, mas que não estão amplamente acessíveis ao público em geral. Um exemplo seria o histórico de consultas médicas que um paciente deseja compartilhar com um grupo de médicos, mas que não deve ser acessado por pessoas fora dessa rede específica. O consentimento do indivíduo é necessário para o compartilhamento desses dados, embora o nível de proteção possa ser inferior ao dos dados totalmente privados.

   i. No caso de Alice: Inclui seu nome, histórico clínico, exames médicos e informações sobre transtornos psicológicos. Esses dados precisam ser protegidos contra acessos indevidos e compartilhamentos não autorizados.

4. **Propósito do Contexto da Tarefa (The Purpose of Task Context - Use/Retention)**: Especifica a finalidade para a qual os dados estão sendo coletados, como serão utilizados e por quanto tempo serão retidos;

   I. No caso de Alice: Os dados de Alice são utilizados para diagnóstico e tratamento, sendo compartilhados entre os profissionais de saúde conforme a necessidade clínica. Alice também espera que seus dados sejam retidos apenas enquanto forem necessários para seu tratamento e que não sejam mantidos indefinidamente pelo Instituto de Pesquisa.

5. **Restrições de Privacidade (Privacy Constraints)**: Define as restrições e obrigações impostas ao processamento dos dados pessoais, como consentimento do usuário, anonimização e políticas de retenção;
    I. No caso de Alice: A usuária impõe restrições específicas ao compartilhamento de seus dados. Por exemplo, ela deseja compartilhar informações apenas para fins de tratamento, garantir que seus dados não sejam acessados por terceiros sem consentimento, e que sejam excluídos quando não forem mais necessários.
6. **Cenário de Risco de Privacidade (Privacy Risk Scenario)**: Modela possíveis ameaças à privacidade, considerando riscos como acessos não autorizados, vazamentos de informações e processamento indevido de dados;
    I. No caso de Alice: Existem riscos de exposição indevida de informações sensíveis, como a possibilidade de um profissional de saúde acessar dados além do necessário ou de o Instituto de Pesquisa armazenar informações além do prazo permitido. Outros riscos incluem vazamentos de dados e acessos não autorizados.
7. **Mecanismos de Privacidade (Privacy Mechanisms)**: Define os controles e mecanismos adotados para mitigar os riscos identificados, incluindo criptografia, autenticação multifator e auditorias de acesso;
    I. No caso de Alice: Essa categoria abrange as medidas implementadas para garantir que os dados sejam tratados de acordo com as restrições de privacidade estabelecidas. O foco está na definição de diretrizes e controles que regulam o acesso, armazenamento e compartilhamento das informações, garantindo que os requisitos de privacidade sejam atendidos de forma estruturada.

A identificação correta dos dados dentro dessas categorias é fundamental para assegurar que os requisitos de privacidade sejam tratados adequadamente, permitindo uma gestão eficaz da segurança e conformidade regulatória.

4. PROPOSTA DE INTEGRAÇÃO

A escolha pela integração do LINDDUN e STRIDE ao PCM justifica-se pela necessidade de ampliar a cobertura analítica da metodologia original. Embora o PCM ofereça uma estrutura robusta para a definição de requisitos de privacidade, ele carece de mecanismos sistemáticos para antecipar ameaças e riscos associados ao uso indevido de dados pessoais. Essa limitação é observada por Peixoto (2021), que destaca a necessidade de mecanismos complementares para apoiar a identificação de ameaças. A análise de riscos de privacidade deve, portanto, considerar abordagens mais completas, como as propostas por Franco et al. (2022), que apontam a importância de integrar modelos de segurança e privacidade para garantir uma proteção mais eficaz. Além disso, a aplicação de diretrizes internacionais, como as previstas nas normas ISO/IEC/IEEE (2018), reforça a necessidade de adotar estratégias que considerem tanto aspectos técnicos quanto regulatórios. A integração proposta amplia a capacidade do PCM de mitigar ameaças emergentes, promovendo uma abordagem estruturada e alinhada às melhores práticas em engenharia de requisitos e segurança da informação.

A modelagem de ameaças no desenvolvimento de software tem se tornado um fator essencial para garantir segurança e conformidade regulatória, especialmente em sistemas que lidam com dados sensíveis. O Privacy Criteria Method (PCM) proposto por Peixoto (2021) tem sido uma abordagem relevante para a especificação de requisitos de privacidade, garantindo um mapeamento detalhado das informações processadas e suas restrições. No entanto, o PCM apresenta limitações quanto aos riscos e mecanismos de privacidade. Para preencher essas lacunas, propõe-se a integração do PCM com as metodologias LINDDUN e STRIDE, ampliando sua capacidade de identificação e tratamento de riscos à privacidade e segurança dos dados.

A integração do LINDDUN e STRIDE ao PCM visa aprimorar a orientação dos usuários na especificação e análise de riscos à privacidade e segurança. O PCM fornece uma estrutura clara para documentar requisitos de privacidade, enquanto o LINDDUN auxilia na identificação de ameaças com base nos fluxos de dados, organizando riscos como vinculabilidade, identificabilidade e divulgação indevida de informações (DENG et al., 2011).

Paralelamente, o STRIDE fortalece a segurança, permitindo que os usuários identifiquem ameaças como falsificação, adulteração e negação de serviço, garantindo que camadas de proteção sejam implementadas adequadamente (Shostack, 2014). Ao unificar essas metodologias, a proposta não apenas amplia a capacidade de identificação e mitigação de riscos, mas também facilita o uso do

PCM, fornecendo diretrizes mais estruturadas para que os usuários tomem decisões informadas e apliquem os requisitos de privacidade de maneira eficiente.

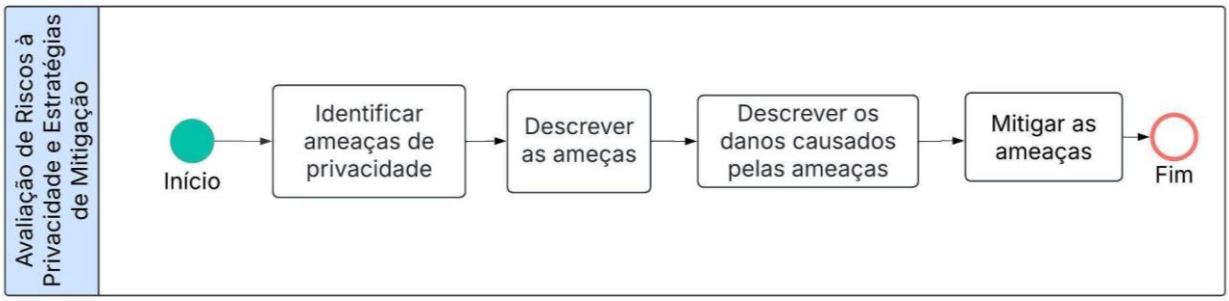
4.1 Aplicação do PCM - Estruturando os Requisitos de Privacidade

O PCM é o alicerce da abordagem. Ele define quem são os atores, quais dados são coletados, como são processados e quais mecanismos de controle devem ser implementados. Essa etapa é fundamental para garantir que a privacidade seja incorporada desde o início do projeto.

A Figura 3 ilustra o processo BPMN revisado para a aplicação dos métodos LINDDUN e STRIDE no PCM. O fluxo começa com a "Identificação das Ameaças de Privacidade", onde as ameaças associadas à privacidade dos dados são analisadas. Em seguida, realiza-se a "Descrição das Ameaças", que avalia as ameaças potenciais que podem comprometer a privacidade dos dados. O próximo passo é a "Descrição dos Danos Causados pelas Ameaças", onde são detalhados os impactos que essas ameaças podem ter sobre a privacidade do usuário. Após isso, a etapa de "Mitigação das Ameaças" é implementada, onde as estratégias para reduzir os riscos identificados são selecionadas.

Vale ressaltar que as ameaças identificadas pelo LINDDUN, que se referem a questões específicas de privacidade, serão mitigadas pelo STRIDE somente se este último, com sua metodologia, for capaz de tratar essas questões. Isso significa que, enquanto o LINDDUN foca em ameaças relacionadas à privacidade, o STRIDE atua em uma camada de segurança mais abrangente e só será aplicado a essas ameaças caso sua metodologia de mitigação de segurança se alinhe com as características do risco identificado. Este fluxo oferece uma abordagem estruturada que garante a proteção de dados, alinhando as melhores práticas de privacidade e segurança para mitigar tanto as ameaças de privacidade quanto as de segurança. Esse processo é essencial para garantir que os dados pessoais sejam tratados de forma segura e em conformidade com as exigências regulatórias.

Figura 3 - Modelagem BPMN da aplicação dos métodos LINDDUN e STRIDE no PCM



4.1.1 Identificação de Ameaças à Privacidade com LINDDUN

Agora que os requisitos de privacidade foram definidos, utilizamos o LINDDUN para mapear ameaças potenciais relacionadas à privacidade. Essa abordagem é estruturada em seis categorias de ameaças (Tabela 10).

Tabela 10 – Ameaças à Privacidade com LINDDUN

Ameaça	**Descrição**
Linkability (Vinculabilidade)	Um invasor pode vincular informações de diferentes fontes e identificar um usuário.
Identifiability (Identificabilidade)	O sistema pode expor a identidade real de um usuário.
Non-repudiation (Não repúdio)	O usuário não pode negar que realizou determinada ação.
Detectability (Detectabilidade)	É possível inferir a presença de um usuário no sistema.
Disclosure of Information (Divulgação de Informações)	Exposição não autorizada de dados
Unawareness (Desconhecimento do Usuário)	Dados podem ser expostos para terceiros não autorizados.

A análise dos riscos de privacidade dentro do PCM é reforçada pelo LINDDUN permite identificar cenários onde os usuários podem ter sua privacidade comprometida. Um dos desafios mais comuns é a falta de conhecimento e controle sobre suas preferências de consentimento, o que pode levar ao uso indevido de seus dados. A tabela 11 a seguir ilustra um exemplo de cenário de risco identificado, destacando ameaças potenciais e os impactos para os titulares dos dados (Tabela 11).

Tabela 11 - Cenário de Risco de Privacidade – PCM

<table>
<tr><td rowspan="4">6 - Privacy Risk Scenario</td><td>Potential Vulnerability</td><td>EXPLORED BY</td><td>Potential Threat</td></tr>
<tr><td>Unawareness and Unintervenability</td><td colspan="2">The data subject is not able to set his/her consent preferences for the processing of personal data.</td></tr>
<tr><td colspan="3">CAUSE</td></tr>
<tr><td colspan="3">Potential Harm</td></tr>
<tr><td colspan="3">The data subject is unable to limit access to their personal data and this data ends up being used against the data subject's will.</td></tr>
</table>

Esse cenário demonstra um problema crítico de Unawareness (Desconhecimento), onde o usuário não possui clareza sobre suas opções de consentimento, resultando no uso de seus dados sem seu pleno controle. Para mitigar esse risco, o sistema deve adotar mecanismos de transparência, garantindo que os indivíduos tenham conhecimento claro sobre como seus dados estão sendo coletados, processados e compartilhados.

Conforme as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2024), é essencial que os sistemas que lidam com informações pessoais forneçam interfaces intuitivas e acessíveis para que os usuários possam gerenciar suas preferências de privacidade de maneira ativa. Isso inclui a implementação de notificações sobre o uso de dados, opções de consentimento granular e mecanismos que possibilitem a revisão e alteração de permissões a qualquer momento. Além disso, a adoção do princípio Privacy by Default assegura que as configurações mais restritivas sejam aplicadas como padrão, reduzindo a exposição desnecessária dos dados do usuário e promovendo um maior alinhamento com regulamentos como a LGPD e a GDPR.

4.1.2 Estratégias de Mitigação

A análise do exemplo da paciente Alice evidencia vulnerabilidades críticas relacionadas à segurança dos dados médicos, que podem comprometer sua integridade, confidencialidade e disponibilidade. A identificação dessas vulnerabilidades foi realizada com base na modelagem de ameaças do STRIDE (Shostack, 2014) e no mapeamento de riscos do Privacy Criteria Method (PCM) (Peixoto, 2021), permitindo uma abordagem estruturada para análise e mitigação de riscos no sistema de saúde;

Dentre as principais falhas identificadas, destaca-se a ausência de autenticação multifator para profissionais de saúde e pesquisadores, permitindo a possibilidade de spoofing, onde um atacante pode se passar por um usuário autorizado para acessar informações sensíveis. A autenticação baseada apenas em senha é vulnerável a ataques de phishing e vazamento de credenciais, tornando essencial a adoção de camadas adicionais de autenticação para garantir que apenas usuários autorizados tenham acesso aos registros médicos (Shostack, 2014).

Além disso, a falta de mecanismos robustos de verificação da integridade dos registros médicos expõe o sistema ao risco de tampering, possibilitando a modificação não autorizada de dados, o que pode comprometer a confiabilidade do diagnóstico e do tratamento. A manipulação indevida de informações médicas pode levar a prescrições incorretas e a um atendimento inadequado ao paciente, sendo essencial implementar mecanismos de rastreamento de alterações e auditoria imutável dos registros (Franco et al., 2022).

A inexistência de um sistema eficaz de auditoria dificulta a rastreabilidade das ações realizadas no sistema, contribuindo para a ameaça de repúdio, onde um usuário pode negar que realizou determinada operação. O registro detalhado de logs com carimbos de data e hora e assinaturas digitais pode garantir a responsabilidade e autenticidade das ações realizadas no sistema, prevenindo fraudes e garantindo conformidade com regulações como a LGPD e GDPR (ISO/IEC/IEEE, 2018).

Outra vulnerabilidade crítica é a exposição dos dados durante a transmissão e armazenamento, devido à ausência de criptografia forte. Isso facilita ataques de exposição de informações, onde dados médicos podem ser interceptados por agentes mal-intencionados. A proteção das informações deve considerar tanto a criptografia em repouso quanto a criptografia em trânsito, garantindo que os dados permaneçam protegidos independentemente do meio de comunicação utilizado (Franco et al., 2022). No que tange à disponibilidade dos serviços, o sistema apresenta riscos de denial of service (DoS), pois não há mecanismos eficazes para mitigar ataques que possam interromper o funcionamento da plataforma, impedindo o acesso dos profissionais aos registros

médicos de Alice. Estratégias como controle de tráfego malicioso e mecanismos de failover podem ser adotadas para garantir a continuidade operacional do sistema em caso de tentativas de sobrecarga (Shostack, 2014).

Por fim, a ausência de um controle adequado de privilégios pode resultar na elevação de privilégios, permitindo que usuários sem autorização obtenham permissões administrativas indevidas e comprometam toda a estrutura de segurança do sistema. A adoção do princípio do menor privilégio, juntamente com a revisão periódica das permissões concedidas, reduz o risco de acessos indevidos e proteger informações sensíveis contra manipulações mal-intencionadas (Franco et al., 2022).

A definição das estratégias de mitigação apresentadas nesta seção seguiu um processo estruturado de análise de ameaças com base no modelo STRIDE, associado à modelagem de requisitos de privacidade do PCM. As ameaças foram identificadas a partir da interação dos atores do sistema com os dados médicos de Alice, e as soluções foram selecionadas com base nas diretrizes de segurança da informação e privacidade estabelecidas na literatura e em normativas reconhecidas (ISO/IEC/IEEE, 2018; Shostack, 2014).

A Tabela 12 apresenta um conjunto de estratégias de mitigação direcionadas exclusivamente para os aspectos de segurança do sistema, destacando medidas técnicas e operacionais que podem ser implementadas para reduzir vulnerabilidades e assegurar um ambiente mais protegido.

Tabela 12 - Estratégias de Mitigação de Ameaças à Segurança

Spoofing (Falsificação de Identidade)	Implementação de autenticação multifator (MFA) para profissionais de saúde e pesquisadores; uso de certificados digitais para autenticação segura.
Tampering (Adulteração de Dados)	Aplicação de assinaturas digitais para garantir a integridade dos registros médicos; utilização de logs imutáveis para rastreamento de modificações.
Repudiation (Repúdio)	Registro detalhado de logs com carimbos de data/hora e assinaturas digitais para garantir a rastreabilidade das operações realizadas no sistema.
Information Disclosure (Exposição de Informações)	Implementação de criptografia de ponta a ponta (E2EE) para a transmissão e armazenamento de dados; controle granular de acesso para restringir visualizações desnecessárias.
Denial of Service (Negação de Serviço - DoS)	Adoção de medidas de mitigação contra ataques DDoS, como limitação de requisições e detecção de tráfego anômalo; redundância da infraestrutura para garantir disponibilidade.
Elevation of Privilege (Elevação de Privilégio)	Aplicação do princípio do menor privilégio, garantindo que usuários tenham apenas as permissões estritamente necessárias; auditoria periódica de acessos e permissões administrativas.

Para garantir a segurança dos dados no caso de Alice, foi aplicada a metodologia STRIDE para identificar e mitigar ameaças ao sistema. Com base nessa análise, foram adotadas medidas de proteção que fortalecem a integridade, confidencialidade e disponibilidade das informações, reduzindo riscos como falsificação de identidade (spoofing), adulteração de dados (tampering) e exposição indevida de informações (information disclosure) (Shostack, 2014). A implementação de mecanismos como autenticação multifator (MFA) para restringir acessos não autorizados, criptografia para proteger dados armazenados e transmitidos, assinaturas digitais para garantir a integridade dos registros médicos, além da aplicação de auditoria de logs e medidas contra ataques DDoS, assegura um ambiente mais seguro e confiável (Franco et al., 2022). A Tabela 13 resume os mecanismos de segurança implementados com base no STRIDE para a mitigação de ameaças.

Tabela 13 - Mecanismos de Privacidade

7 - Privacy Mechanisms (Mecanismos de Privacidade)	**Autenticação Multifator (MFA)**: Restrição de acesso apenas a usuários autorizados; **Criptografia**: Proteção dos dados armazenados e transmitidos; **Assinaturas Digitais**: Garantia de integridade dos registros médicos; **Proteção contra DDoS**: Detecção e mitigação de tráfego anômalo; **Controle de Privilégios**: Permissões mínimas para cada usuário.

5. ANÁLISE DA APLICAÇÃO DO PCM + LINDDUN NOS ARTEFATOS

Para validar a implementação do Privacy Criteria Method (PCM) integrado ao LINDDUN, foram analisados artefatos desenvolvidos por 17 alunos da disciplina de Engenharia de Requisitos, do curso de Sistemas de Informação da Universidade Federal de Pernambuco, no período letivo de 2024.2. Dois times produziram artefatos do PCM, totalizando 17 artefatos. Nessas produções, foram aplicados os princípios do PCM e do LINDDUN para especificar requisitos de privacidade e identificar ameaças de privacidade de dados nos sistemas avaliados.

A análise desses artefatos teve como objetivo verificar se os princípios do LINDDUN foram corretamente aplicados para a identificação de ameaças à privacidade, garantindo que os riscos fossem devidamente categorizados e que medidas apropriadas fossem propostas dentro do escopo do PCM. Para tal verificação, foram estabelecidos critérios de qualidade, que permitiram avaliar a adequação dos artefatos às diretrizes do modelo. As tabelas 14 e 15 apresentam a relação dos artefatos analisados e os resultados da avaliação, conforme os critérios definidos.

Durante a análise dos artefatos desenvolvidos pelos alunos, verificou-se que o modelo LINDDUN foi aplicado para a identificação de riscos à privacidade, enquanto o STRIDE, voltado para ameaças à segurança da informação, não foi incorporado à avaliação realizada nesta fase do estudo. No entanto, a inclusão do STRIDE na análise dos artefatos é uma etapa fundamental para aprimorar a abordagem de mitigação de riscos, pois permitirá a identificação de ameaças (Hossain e Hassan, 2023).

Dessa forma, trabalhos futuros poderão explorar a aplicação do STRIDE nesses mesmos artefatos, permitindo uma abordagem combinada de segurança e privacidade. A integração dos dois modelos possibilitará uma análise mais robusta dos riscos enfrentados pelos sistemas avaliados, garantindo maior proteção dos dados e conformidade com regulamentações como a LGPD e GDPR (Martin e Kung, 2018).

Os seguintes critérios foram definidos para avaliar a aplicação do PCM + LINDDUN nos artefatos:

1. **Identificação correta das ameaças (LINDDUN**): O artefato reconhece corretamente as ameaças de privacidade, como linkabilidade, identificabilidade e exposição de dados;
2. **Correspondência entre as ameaças e mecanismos de mitigação:** O artefato propõe mecanismos apropriados para cada ameaça identificada;

3. **Aplicação adequada das diretrizes do PCM**: O artefato segue as diretrizes do PCM para a proteção de dados e implementação de boas práticas de segurança;
4. **Clareza e completude:** O artefato apresenta informações organizadas, detalhadas e compreensíveis;
5. **Conformidade com regulamentações:** O artefato demonstra preocupação com a conformidade legal, incluindo medidas como consentimento, anonimização e transparência.

5.1 Artefatos Relacionados à Exportação de Relatórios e Gestão de Dados

Este grupo especificou 9 artefatos voltados para a exportação de relatórios e gestão de dados, abordando funcionalidades como exportação de arquivos, criação de relatórios e controle de formulários. A aplicação do PCM com a metodologia LINDDUN nesses artefatos buscou identificar riscos de privacidade relacionados ao acesso a dados, rastreabilidade de atividades e proteção contra vazamentos de informações.

A análise revelou que a maioria dos artefatos identificou corretamente ameaças como Linkability, Identifiability e Information Disclosure, mas houve inconsistências na definição de mecanismos de mitigação e na implementação de controles adequados para evitar exposição indevida de informações.

Tabela 14 - Avaliação dos Artefatos de Exportação de Relatórios e Gestão de Dados

ID do Artefato	Identificação Correta das Ameaças	Correspondência entre Ameaças e Mitigação	Aplicação Adequada do PCM	Clareza e Completude	Conformidade com LGPD/GDPR	Resultado Geral
PC01	✅	✅	⚠️	✅	⚠️	Parcialmente Correto
PC02	✅	✅	✅	✅	✅	Correto
PC03	⚠️	✅	✅	✅	⚠️	Parcialmente Correto
PC04	✅	⚠️	✅	⚠️	✅	Parcialmente Correto
PC05	✅	✅	✅	✅	✅	Correto
PC06	⚠️	✅	⚠️	✅	⚠️	Parcialmente Correto
PC07	✅	✅	✅	✅	✅	Correto
PC08	⚠️	✅	⚠️	✅	⚠️	Parcialmente Correto
PC09	✅	✅	✅	✅	✅	Correto

Legenda: ✅ Correto | ⚠️ Parcialmente Correto | ❌ Não Aplicado

5.1.2 Análise do Grupo de Exportação de Relatórios e Gestão de Dados

I. **PC01**;

a. Erro: O artefato apresentou fragilidades na aplicação adequada do PCM, especialmente na definição de controles de acesso;

b. Recomendação: Incluir mecanismos como autenticação forte, restrição de acesso por perfis e rastreamento de acessos para garantir maior proteção.

II. **PC03**;
    a. Erro: A identificação das ameaças não foi completamente correta, e a conformidade com LGPD/GDPR não foi plenamente abordada;
    b. Recomendação: Ampliar a análise de riscos, considerando ameaças negligenciadas, como Information Disclosure e Repudiation. Além disso, detalhar políticas de retenção de dados e consentimento para garantir conformidade regulatória.

III. **PC04**;
    a. Erro: A correspondência entre ameaças e mitigação apresentou inconsistências, e a clareza na documentação dos requisitos foi comprometida;
    b. Recomendação: Garantir que cada ameaça identificada tenha um mecanismo de mitigação claro, evitando soluções genéricas. Melhorar a documentação da análise para facilitar a interpretação dos resultados.

IV. **PC06**;
    a. Erro: Houve falhas tanto na identificação das ameaças quanto na aplicação correta do PCM. Além disso, a conformidade regulatória foi tratada de forma superficial;
    b. Recomendação: Rever o mapeamento de ameaças e garantir que todas as categorias do LINDDUN sejam analisadas. Melhorar a descrição das políticas de privacidade e retenção de dados.

V. **PC08**;
    a. Erro: Apresentou falhas na identificação das ameaças, na implementação do PCM e na conformidade com a LGPD/GDPR;
    b. Recomendação: Fortalecer a categorização das ameaças utilizando a metodologia do LINDDUN de forma mais estruturada. Garantir que a documentação de conformidade regulatória esteja alinhada às diretrizes de proteção de dados.

5.2 Artefatos Relacionados à Pegada de Carbono de Pequenas e Médias Empresas (PMEs)

Este grupo contém 8 artefatos voltados para o cálculo da pegada de carbono de Pequenas e Médias Empresas (PMEs). Esses artefatos tratam informações operacionais sensíveis e visam garantir conformidade com regulamentações ambientais e de proteção de dados.

A aplicação do PCM com a metodologia LINDDUN nesses artefatos demonstrou uma preocupação com a segurança e privacidade dos dados corporativos, mas alguns

apresentaram fragilidades na definição de períodos de retenção de dados e anonimização das informações compartilhadas.

Tabela 15 - Avaliação dos Artefatos de Exportação de Relatórios e Gestão de Dados

ID do Artefato	Identificação Correta das Ameaças	Correspondência entre Ameaças e Mitigação	Aplicação Adequada do PCM	Clareza e Completude	Conformidade com LGPD/GDPR	Resultado Geral
PC01	✅	✅	⚠	✅	⚠	Parcialmente Correto
PC02	✅	✅	✅	✅	✅	Correto
PC03	✅	⚠	✅	✅	✅	Parcialmente Correto
PC04	✅	✅	✅	✅	✅	Correto
PC05	⚠	✅	✅	⚠	✅	Parcialmente Correto
PC06	✅	✅	✅	✅	✅	Correto
PC07	✅	✅	✅	✅	✅	Correto
PC08	⚠	✅	⚠	✅	⚠	Parcialmente Correto

Legenda: ✅ Correto | ⚠ Parcialmente Correto | ❌ Não Aplicado

5.2.1 Análise da Pegada de Carbono de Pequenas e Médias Empresas (PMEs)

I. **PC10;**

   a. **Erro**: O artefato não detalhou como garantir o consentimento explícito das empresas no uso dos dados;

   b. **Recomendação**: Incluir termos de consentimento e notificações claras sobre o uso e compartilhamento das informações.

II. **PC12**;
    a. **Erro**: A relação entre ameaças identificadas e mecanismos de mitigação não foi plenamente explicada;
    b. **Recomendação**: Especificar melhor como cada ameaça identificada será mitigada, detalhando os controles necessários.
III. **PC14**;
    a. **Erro**: Houve falha na clareza e completude das informações, comprometendo a interpretação do artefato;
    b. **Recomendação**: Melhorar a documentação e a organização dos requisitos, garantindo que as ameaças e suas mitigações sejam explicadas de maneira objetiva e estruturada.
IV. **PC17**;
    a. **Erro**: Apresentou deficiências na identificação de ameaças, na aplicação correta do PCM e na conformidade regulatória;
    b. **Recomendação**: Rever o mapeamento de ameaças, garantir que todos os aspectos da LGPD/GDPR sejam contemplados e melhorem a clareza dos requisitos de privacidade.

A análise dos artefatos desenvolvidos pelos alunos foi conduzida com base em critérios claros para avaliar a aplicação do PCM integrado ao LINDDUN, focando principalmente na identificação correta das ameaças, a correspondência entre ameaças e mitigações, a clareza e completude das informações, e a conformidade com regulamentações como a LGPD/GDPR. Durante a análise, constatou-se que, de um total de 17 artefatos, 9 apresentaram algumas falhas. Essas falhas estavam relacionadas principalmente à definição e implementação de mecanismos de mitigação, à clareza da documentação e à consideração completa dos aspectos regulatórios. As recomendações para esses artefatos indicaram a necessidade de aprimoramento na conexão entre ameaças e suas contramedidas, além de melhorias na descrição das políticas de privacidade e maior detalhamento nas diretrizes de conformidade regulatória.

Com relação ao aprendizado dos alunos, a aplicação do PCM integrado ao LINDDUN foi, em sua maioria, bem-sucedida. A análise indicou que a maioria dos artefatos (8 de 17) apresentou a aplicação correta dos conceitos e das metodologias, refletindo um bom entendimento do modelo. No entanto, 9 artefatos ainda necessitam de ajustes para atingir um nível de aplicação totalmente adequado, principalmente no que se refere à documentação e à ligação entre ameaças e mitigações. Dessa forma, apesar de bons avanços, alguns pontos ainda precisam ser trabalhados para garantir que

todos os artefatos atendam de forma plena às diretrizes do PCM juntamente com a modelagem LINDDUN.

6. CONCLUSÃO

A integração do PCM às abordagens modeladoras LINDDUN e STRIDE enriquece de forma marcante a descrição e mitigação dos riscos de privacidade e segurança, superando as inadequações inerentes às metodologias tradicionais. O modelo resultante permite que se trate de forma sistemática e minuciosa os requisitos de segurança e privacidade; assim, ele garante alinhamento com as leis, como a LGPD e a GDPR, além de aumentar a resiliência dos sistemas a ameaças.

A soma dessas abordagens cria um arcabouço metodológico robusto e inovador enquanto que o PCM serve como a estrutura para a definição de requisitos de privacidade, o LINDDUN possibilita a identificação de ameaças à privacidade, que é realizada por meio da modelagem dos fluxos de dados, assim, as ameaças em risco seriam identificáveis em vínculos, identificação e disponibilidade indesejada de informações (Deng et al., 2011). De forma complementar, o STRIDE proporciona uma camada de análise de segurança, tratando ameaças como falsificação, adulteração, repúdio e negação de serviço, garantindo que os ataques cibernéticos e vulnerabilidades sejam mitigáveis desde as primeiras fases de desenvolvimento do próprio sistema (Shostack, 2014).

Essa integração, além de proporcionar uma segurança adicional dos dados, atenua o processo de incorporação das estratégias de Privacy by Design e Security by Design, permitindo a aplicação de controles de segurança desde o desenvolvimento do sistema. Privacy by Design garante que a privacidade seja considerada em todas as etapas do ciclo de vida do software, atendendo às exigências regulatórias e reduzindo riscos associados à exposição indevida de informações (Martin e Kung, 2018). Já o conceito de Security by Design enfatiza a implementação de medidas de proteção contra ameaças desde a concepção do sistema, fortalecendo sua resiliência contra ataques e falhas de segurança (Anderson, 2010).

Dessa forma, os sistemas tornam-se compatíveis não apenas com as pautas legais, mas também com padrões técnicos complexos que mitigam os riscos operacionais, garantindo confidencialidade, integridade e disponibilidade das informações.

A validade desta aproximação pode ser confirmada por seu uso no estudo ilustrativo de Alice, que demonstrou que a interseção do PCM, o LINDDUN pode proporcionar um método estruturado para a descrição e mitigação de ameaças. O uso da metodologia permitiu mapear

vulnerabilidades no fluxo de dados de saúde, detectar pontos vulneráveis de privacidade e sugerir contramedidas. Portanto, a proposta apresentada pode avançar o estado da arte da Engenharia de Requisitos, fornecendo um modelo mais claro e eficaz para o desenvolvimento de sistemas que atendam aos requisitos regulatórios e possuam uma proteção robusta contra ameaças. Essa integração contribui para a construção de sistemas mais seguros, transparentes e confiáveis, essenciais em um cenário de crescente digitalização e compartilhamento de dados sensíveis.

6.1. Discussão e Trabalhos Futuros

A integração do PCM com os métodos LINDDUN e STRIDE representa uma abordagem promissora para o aprimoramento da especificação e mitigação de riscos à privacidade e à segurança. Ao longo deste estudo, foi demonstrado que essa combinação possibilita uma análise estruturada de ameaças, garantindo maior alinhamento com regulamentações como LGPD e GDPR. No entanto, apesar das contribuições obtidas, ainda é necessário avaliar a abordagem de forma completa, incluindo a aplicação do STRIDE, o que não foi possível neste semestre devido a restrições de escopo da disciplina. Essa análise mais abrangente permitirá validar a efetividade da integração entre os três métodos em um contexto real e mais diversificado. Assim, pesquisas futuras poderão aprofundar a implementação do STRIDE e integrar completamente os dois modelos, proporcionando uma análise mais robusta de segurança e privacidade.

Uma das principais perspectivas é a aplicação da metodologia em um conjunto maior de cenários ilustrativos, permitindo uma análise comparativa mais ampla sobre os impactos da integração. Essa abordagem possibilitará avaliar como o modelo se adapta a diferentes domínios, como, financeiro, e-commerce e administração pública, garantindo que suas diretrizes sejam suficientemente flexíveis e eficazes para sistemas de diversas complexidades e requisitos regulatórios.

Ademais, é fundamental expandir a investigação para além das estratégias de mitigação de riscos associadas ao STRIDE, pois há ameaças à privacidade que não estão diretamente relacionadas com falhas de segurança, mas com questões regulatórias e de conformidade. Por exemplo, não conformidade, não repúdio e linkabilidade são ameaças que afetam a privacidade, mas não necessariamente estão ligadas a vulnerabilidades de segurança no sistema. Portanto, a aplicação de mecanismos de privacidade deve ser ampliada para abordar essas questões de forma eficaz. Futuras pesquisas devem focar no desenvolvimento de estratégias que integrem esses aspectos de privacidade, permitindo que o modelo ofereça uma abordagem mais completa para a proteção de dados pessoais, alinhada tanto com os requisitos de segurança quanto com as demandas regulatórias e éticas.

Outro aspecto relevante para validação da proposta é a realização de um survey com especialistas da área de segurança e privacidade. Essa pesquisa permitiria coletar feedback de profissionais e pesquisadores sobre a aceitação e aplicabilidade do modelo no mercado. Especialistas poderiam avaliar a facilidade de implementação da abordagem, sua compatibilidade com práticas de Engenharia de Requisitos já consolidadas e potenciais desafios na sua adoção em projetos reais. Esse estudo também poderia fornecer insights sobre possíveis ajustes e melhorias.

REFERÊNCIAS

Anderson, J. **Security engineering**: a guide to building dependable distributed systems. John Wiley & Sons, 2010.

Boehm, W. **Software engineering economics**. Springer Berlin Heidelberg, 2002.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 mar. 2025.

Cellard, A. **"A análise documental."** In: A pesquisa qualitativa: enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008. p. 295-316.

Deng, M, et al. **A privacy threat analysis framework**: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering, v. 16, n. 1, p. 3-32, 2011.

GDPR.EU. **The EU general data protection regulation**. 2018. Disponível em:. Diretrizes gerais de conformidade com o GDPR (Regulamento Geral de Proteção de Dados) Acesso em: 8 mar. 2025.

Franco, F; Lacerda, M. Stiller, B. **A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises**. Revista de Gestão e Projetos, v. 13, n. 3, p. 10-37, 2022.

Gil, C. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

Hossain, I. Hasan, R. **Improving Security Practices in Health Information Systems with STRIDE Threat Modeling.** In: IEEE 9th World Forum on Internet of Things (WF-IoT). IEEE, 2023. p. 1-6.

Ilg, Manuel. Rieger, V. Angermeier, D. **A Systematic Approach to Modeling Software-Defined Vehicles and their Security Needs**. In: AmE Automotive meets Electronics; 14. GMM Symposium. VDE, 2023. p. 68-72.

ISO/IEC/IEEE 29148:2018. **Systems and software engineering — Life cycle processes — Requirements engineering**. 2. ed. International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronics Engineers, 2018.

Kohnfelder, L. Praerit, G. **"The threats to our products."**. Microsoft Interface. Microsoft Corporation 33 (1999).

Liebel, G. Knauss, E. **Aspects of modelling requirements in very-large agile systems engineering. Journal of Systems and Software**, v. 199, p. 111628, 2023.

Marconi, A. Lakatos, M. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

Martin, S. Kung, A. **Methods and tools for GDPR compliance through privacy and data protection engineering**. In: 2018 IEEE European symposium on security and privacy workshops (EuroS&PW). IEEE, 2018. p. 108-111.

Menegazzi, C. **Conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução**. In: Workshop em Engenharia de Requisitos (WER23). 2023.

Nissenbaum, H. **Privacy as contextual integrity**. Wash. L. Rev. v. 79. p. 119. 2004.

Nweke, O, et al. **A LINDDUN-Based Privacy Threat Modelling for National Identification Systems**. In: 2022. Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON). IEEE, 2022. p. 1-8.

OECD. **Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data**. 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 06 jan. 2025.

OWASP Foundation. **Processo de modelagem de ameaças**. Disponível em: https://owasp.org/wwwcommunity/Threat_Modeling_Process#stride-threat-list. Acesso em: 07 jan. 2025.

Parker, B. **Toward a new framework for information security?**. Computer security handbook, p. 3.1-3.23, 2012.

Peixoto, M. **A privacy requirements specification method for Agile Software Development based on exploratory studies**. Programa de Pós-Graduação em Ciência da Computação. Recife, 2021. Disponível em: TESE Mariana Maia Peixoto.pdf. Acesso em: 16 mar. 2025.

Robertson, S. Robertson, J. **Mastering the requirements process**: Getting requirements right. Addison-wesley, 2012.

Severino, J. **Metodologia do trabalho científico**. Cortez editora, 2017.

Sommerville, I. **Software Engineering**, 9/E. Pearson Education India, 2011.

Shostack, A. **Threat modeling**: Designing for security. John Wiley & Sons, 2014.

Souza, L, et al. **Desafios e Práticas da Engenharia de Requisitos no Contexto de Fábrica de Software com foco na Documentação e Gestão do Conhecimento**. Cadernos do IME-Série Informática, v. 42, p. 98-98, 2019.

Van Landuyt, D. Joosen, W. **A descriptive study of assumptions made in LINDDUN privacy threat elicitation**. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing. 2020. p. 1280-1287.

Warren, S. Brandeis, L. **"O direito à privacidade"**, Harvard Law Rev. vol. 4. n. 5. p. 193-220. 1890.

Westin, F. **Privacy and freedom**. Washington and Lee Law Review, v. 25, n. 1, p. 166, 1968.

Whitman, E, et al. **Principles of information security**. Boston, MA: Thomson Course Technology, 2009.

Yin, K. **Case study research and applications**. 2018.

CASARIN, H. D. C. S.; CASARIN, S. J. **Pesquisa científica: da teoria à prática**. Curitiba: InterSaberes, 2012.

WAINER, J. et al. **Métodos de pesquisa quantitativa e qualitativa para a ciência da computação**. Atualização em informática, Sociedade Brasileira de Computação/Editora PUC Rio Rio de Janeiro, v. 1, p. 221–262, 2007.

WAGNER, Stefan et al. **Status quo in requirements engineering: A theory and a global family of surveys**. ACM Transactions on Software Engineering and Methodology (TOSEM), v. 28, n. 2, p. 1-48, 2019.