# Uma Ferramenta Semi-Automatizada de Detecção de Ameaças à Privacidade com LINDDUN PRO

# A Semi-Automated Privacy Threat Detection Tool with LINDDUN PRO

# Una Herramienta Semiautomática de Detección de Amenazas a la Privacidad con LINDDUN PRO

Henrique Mendes[1]
Robson Medeiros[2]

**Resumo:** Aprimorar a privacidade é um desafio crucial no desenvolvimento de software. Metodologias de modelagem de ameaças podem auxiliar na identificação e mitigação de riscos, mas frequentemente são complexas e demoradas. Este artigo apresenta uma ferramenta de modelagem de ameaças semi automatizada baseada na metodologia LINDDUN PRO. A ferramenta, utilizando regras de produção, identifica automaticamente ameaças à privacidade a partir de um diagrama de fluxo de dados. Os resultados da avaliação mostram que a ferramenta efetivamente identifica ameaças à privacidade, sendo uma ferramenta valiosa para desenvolvedores em busca de aprimorar a proteção da privacidade em seus sistemas de software.

**Palavras-chave:** Privacidade. Privacidade por Definição. Segurança. Modelagem de Ameaças. LINDDUN.

**Abstract:** Improving privacy is a critical challenge in software development. Threat modeling methodologies can aid in identifying and mitigating privacy risks, but they often prove complex and time-consuming. This article introduces a semi-automated threat modeling tool based on the LINDDUN PRO methodology. The tool, employing production rules, automatically identifies privacy threats from a data flow diagram. The software evaluation results demonstrate its capability in identifying privacy threats, making it a valuable tool for developers aiming to enhance privacy protection in their software systems.

**Keywords:** Privacy. Privacy by Design. Security. Threat Modeling. LINDDUN.

**Resumen:** Mejorar la privacidad es un desafío crucial en el desarrollo de software. Las metodologías de modelado de amenazas pueden ayudar a identificar y mitigar riesgos de privacidad, pero a menudo resultan complejas y llevan tiempo. Este artículo presenta un software de herramienta de modelado de amenazas semi automatizada basada en la metodología LINDDUN PRO. La herramienta, utilizando reglas de producción, identifica automáticamente amenazas a la privacidad a partir de un diagrama de flujo de datos. Los resultados de la evaluación del software demuestran su capacidad para identificar amenazas a la privacidad, convirtiéndo en una herramienta valiosa para desarrolladores que buscan mejorar la protección de la privacidad en sus sistemas de software.

**Palabras-clave:** Privacidad. Privacidad por diseño. Seguridad. Modelado de Amenazas. LINDDUN.

[1] Graduando em Ciência da Computação. Universidade Federal Rural de Pernambuco. https://orcid.org/0009-0007-0364-357X. E-mail: henrique.mendes@ufrpe.br
[2] Doutor em Ciência da Computação. Universidade Federal Rural de Pernambuco. https://orcid.org/0000-0001-5870-1510. E-mail: robson.medeiros@ufrpe.br.

## Introdução

Com o software presente em vários aspectos da vida atual, dados e privacidade são essenciais para a confiança e a segurança dos usuários. As tecnologias e a digitalização trazem desafios complexos para a privacidade de dados. Por isso, é urgente integrar leis, normas de proteção de dados e privacidade desde o princípio do desenvolvimento de software.

É fundamental, especialmente nas etapas iniciais do desenvolvimento de software, que as legislações e normativas focadas na proteção de dados e privacidade sejam reforçadas por diretrizes práticas. Essas orientações devem prover suporte aos desenvolvedores de software, para superar os desafios inerentes à preservação de privacidade (Alshammari; Simpson, 2017). Influenciada por uma gama de fatores, incluindo não só as transformações das demandas sociais, como também os progressos na tecnologia, a própria natureza subjetiva da privacidade não pode ser adequadamente garantida através apenas de regulamentos (Spiekermann, 2012).

As estratégias sistemáticas de modelagem de ameaças desempenham um papel crucial ao orientar os profissionais na adoção de melhores práticas e na tomada de decisões (McGraw, 2006). Segundo o Instituto Nacional de Padrões e Tecnologia (NIST), a modelagem de ameaças é uma abordagem de avaliação de riscos que busca representar tanto a perspectiva ofensiva quanto defensiva de uma entidade lógica específica, que pode incluir sistemas, ambientes, aplicativos, servidores, elementos de dados ou informações (Souppaya; Scarfone, 2016). A modelagem de ameaças, como parte essencial da segurança cibernética, está se tornando cada vez mais comum na elaboração de aplicativos e na análise de sistemas (Xiong; Lagerström, 2019).

Diversas metodologias, estruturas e ferramentas de modelagem de ameaças foram desenvolvidas, algumas mais abrangentes e outras mais especializadas (Selin, 2019). Uma das metodologias mais conhecidas é a STRIDE (Tuma *et al.*, 2017), consiste em um método que permite identificar ameaças de segurança – seu nome é um acrônimo possuindo seis categorias de ameaças distintas: *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service* e *Elevation of Privilege*. Cada uma dessas classes representa uma violação de uma propriedade desejável para um sistema, como autenticidade, integridade, confidencialidade, disponibilidade e autorização.

A metodologia STRIDE destaca-se na identificação de vulnerabilidades de segurança em sistemas de software (Torr, 2005) e é amplamente aplicada, especialmente nos produtos da Microsoft (Hernan *et al.*, 2016). Por outro lado, a metodologia LINDDUN é uma das

principais referências na esfera da privacidade (Deng *et al.*, 2010), sendo empregada para identificar violações neste contexto (Wuyts, 2015).

Tendo uma evolução notável em uma nova versão chamada LINDDUN PRO (Sion; Joosen, 2023), apresenta uma documentação mais robusta incluindo uma descrição detalhada de cada categoria de ameaça, árvores de ameaças, critérios de privacidade e uma nova tabela de mapeamento. Sustentando-se em uma abordagem baseada em interação de fluxo (fonte, transferência e destino), em vez de se concentrar apenas nos tipos de elementos como era feito na versão anterior.

Baseando-se em uma representação abstrata conhecida como Diagrama de Fluxo de Dados (DFD) (DeMarco, 1981), as técnicas de modelagem de ameaças proporcionam uma análise minuciosa da segurança e privacidade do sistema em fase de projeto (Sion, 2018). No entanto, avaliar ameaças e suas consequências pode ser um processo demorado, especialmente quando incorporado ao desenvolvimento ágil, o que gera desafios significativos (Kunz *et al.*, 2023; Keramati; Mirian-Hosseinabadi, 2008; Galvez; Gurses, 2018). Outrossim, uma revisão da literatura revelou que não há ferramentas disponíveis que automatizem o processo de detecção de ameaças utilizando a metodologia LINDDUN PRO.

Este trabalho propõe uma ferramenta de detecção de ameaças semi automatizada, baseada nas árvores de ameaças catalogadas pelo método LINDDUN PRO (Sion; Joosen, 2023), e utilizando um sistema de regras de produção (Fowler, 2010), para mapear ameaças e identificar automaticamente potenciais riscos à privacidade durante o ciclo de vida do desenvolvimento de software.

**Organização do Trabalho**

Este trabalho é organizado da seguinte forma. Primeiramente são introduzidos conceitos chaves sobre privacidade e modelagem de ameaças. Em seguida, é descrito sobre a metodologia LINDDUN PRO. Na seção seguinte, são discutidos os trabalhos relacionados apresentando e comparando algumas metodologias de modelagem de ameaças e as suas limitações. Nas seções adiantes, além da proposta de solução, também é feita uma descrição de como a arquitetura é representada, detalhando seus principais componentes. Na próxima seção, é feita uma avaliação com um sistema na área de saúde – utilizando a solução proposta por este trabalho, apresentando não só algumas imagens da ferramenta, como também classificação dos critérios de privacidade considerados pela avaliação e expondo como resultado as ameaças encontradas no sistema avaliado. Finalizando com a seção de

considerações finais, onde é apresentado as conclusões do trabalho, as contribuições, as limitações e as sugestões para trabalhos futuros.

**Privacidade**

A definição de privacidade é um dos conceitos mais desafiadores entre os direitos humanos internacionalmente catalogados (Michael, 1994). Na era contemporânea, o conceito se estabeleceu como um dos direitos mais significativos (Rotenberg, 2000). Uma das definições mais conhecidas é a descrição da privacidade como "O direito de ser deixado em paz" (Warren; Brandeis, 1890, p.193).

Com a proliferação de dados pela Internet, surge uma preocupação significativa sobre como esses dados devem ser tratados (Bertino, 2016). Neste contexto, a privacidade de dados não se limita apenas ao direito das pessoas em controlar quem pode acessar seus dados, mas também abrange quais dados serão compartilhados e a segurança dessas informações contra acesso não autorizado (Alafaa, 2022).

No cenário de software, surge um conceito chamado de privacidade por definição, cujo objetivo é adotar medidas proativas em detrimento de reativas. Este conceito tem o intuito de prever e evitar situações invasivas à privacidade antes de sua ocorrência (Cavoukian, 2009). Ao invés de a privacidade ser encarada como um componente extra, um dos princípios fundamentais ressalta a necessidade de incorporar a privacidade durante todo o ciclo de desenvolvimento de software (Wuyts, 2015).

**Modelagem de Ameaças**

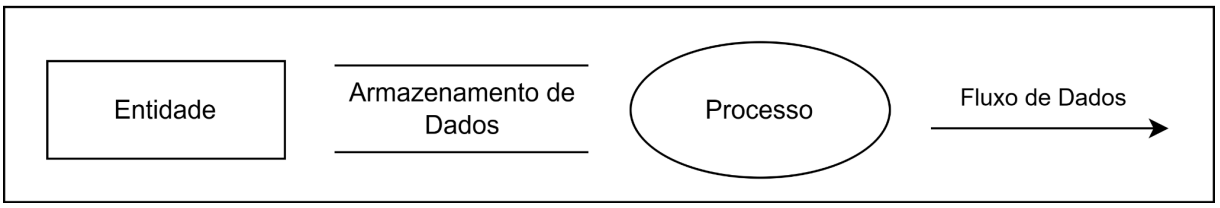
O objetivo da Modelagem de Ameaças é identificar vulnerabilidades de segurança em um sistema, avaliar seu risco, propor medidas de mitigação e acompanhar sua implementação (Yskout *et al.*, 2020). Como mencionado por Shostack (2014), a técnica de modelagem de ameaças consiste na combinação de quatro perguntas chaves: O que está sendo construído? O que pode dar errado? O que se deve fazer sobre as coisas que podem dar errado? Realmente foi feito um bom trabalho de análise?

O uso de um diagrama de fluxo de dados torna-se presente para representar graficamente um sistema e fazer a modelagem de ameaças do mesmo. Diagrama de fluxo de dados (DFDs) é um tipo de estrutura com várias conexões que representa o fluxo de um sistema (DeMarco, 1981).

Os diagramas são gráficos multidimensionais e particionados que enfatizam o fluxo de dados e desfavorecem o fluxo de controle (DeMarco, 1981). Os DFDs permitem uma representação da situação sob a perspectiva dos dados, independentemente de usuários ou organizações envolvidas (DeMarco, 1981).

Na perspectiva da metodologia LINDDUN PRO, os DFDs possuem 4 tipos de elementos, denominados de Fluxo de dados, Armazenamento de dados, Processos e Entidades externas.

Figura 1 – Elementos de um Diagrama de Fluxo de Dados - LINDDUN




Fonte: Adaptado de Wuyts (2015).

A Figura 1 denota a representação de como cada elemento no diagrama de fluxo de dados deve ser representado. Cada elemento possui um significado:

- Entidade: Usuários ou serviços de terceiros externos ao sistema.
- Armazenamento de Dados: Onde os dados podem ser armazenados.
- Processos: Unidades de computação.
- Fluxos de Dados: Sentido do fluxo da informação pelo sistema.

O DFD é a base da análise de ameaças, pois cada um de seus elementos é minuciosamente investigado de forma sistemática em busca de ameaças à privacidade (Wuyts, 2015).

**LINDDUN PRO**

LINDDUN é uma metodologia de modelagem de ameaças que tem o objetivo de auxiliar os desenvolvedores a identificar e resolver os problemas de privacidade em suas aplicações. Através de uma análise do software, procura-se quaisquer potenciais desafios relacionados à privacidade (Wuyts, 2015).

O nome da metodologia é um acrônimo baseado nas categorias de ameaça: *Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness &*

*Unintervenability* e *Non-compliance*. Durante a fase inicial, o LINDDUN permite identificar deficiências de design relacionadas à privacidade, tornando possível um framework de modelagem de ameaças focado em categorias específicas de ameaças à privacidade (Scandariato *et al.*, 2013).

*Linkability* (Vinculação de dados) é a conexão de dados diferentes para revelar informações adicionais sobre um indivíduo ou grupo, comprometendo a privacidade. Isso geralmente ocorre por meio de um identificador repetido, características combinadas ou um perfil que separa os dados (Sion; Joosen, 2023);

*Identifiability* (Identificação), que se refere à categoria de que as informações pessoais estão intrinsecamente relacionadas a um indivíduo específico, cuja identidade pode ser revelada por meios não autorizados, inferida, ou até mesmo presumida (Sion; Joosen, 2023);

*Non-Repudiation* (Não repúdio) é quando alguém não pode negar afirmações, especialmente sobre sua participação no sistema ou declarações relacionadas a ela. Isso ocorre devido a dados coletados, divulgados ou ações realizadas no sistema (Sion; Joosen, 2023);

*Detectability* (Detecção) é a consciência da participação do sujeito de dados no sistema ao notar informações relevantes, como comunicação observada, efeitos na aplicação ou respostas do sistema (Sion; Joosen, 2023);

*Data Disclosure* (Divulgação de Dados) é a divulgação, coleta excessiva ou acidental de informações pessoais, representando uma ameaça à privacidade (Sion; Joosen, 2023);

*Unawareness & Unintervenability* (Desconhecimento e Falta de Intervenção) são a falta de suporte para pessoas afetadas por um sistema, causando danos à privacidade devido à insuficiência em informar, envolver ou habilitar adequadamente o indivíduo em sua função e interação com o sistema (Sion; Joosen, 2023);

*Non-Compliance* (Não Conformidade) trata-se da não aderência de leis, regulamentos, normas e contratos, resultando em gestão inadequada de riscos, especialmente em operações de processamento de dados que não estão em conformidade com regulamentações de privacidade (Sion; Joosen, 2023).

A metodologia tradicional recebeu uma nova versão, chamada de LINDDUN PRO – sendo conhecido por LINDDUN-per-interaction (LINDDUN PRO, 2024). Diferente da primeira versão, onde é dirigida aos tipos de elementos no DFD, por outro lado a versão PRO tem foco na comunicação, bem como é dirigida ao fluxo de interação. É importante ressaltar que a antiga metodologia baseava-se apenas nos elementos, no entanto, esse tipo de abordagem apresenta uma desvantagem significativa, pois não considera informações

contextuais, desde o elemento de envio ou o recebimento de informações, ou o tipo do outro elemento com o qual se comunica (Sion, 2020).

A metodologia LINDDUN PRO possui alguns componentes necessários (Sion; Joosen, 2023), como as árvores de ameaças, onde baseiam-se nos avanços no campo da proteção de dados e da segurança da informação. Elucidam padrões mais usuais em cada categoria de ameaças e estimulam os desenvolvedores de software na avaliação de possíveis ameaças relacionadas à privacidade em seu sistema (Wuyts, 2015). Na metodologia LINDDUN PRO, há várias versões das árvores de ameaças, cada uma oferecendo uma quantidade diferente de informações. Isso permite a escolha da versão na qual melhor atenda às necessidades, seja ela básica, com exemplos, ou com critérios de privacidade, impacto e informações adicionais (Sion; Joosen, 2023). Uma das vantagens significativas do LINDDUN PRO consiste na atualização e melhoria de suas árvores de ameaças, bem como na inclusão de critérios focados em privacidade que possibilitam compreender melhor se alguma ameaça é aplicável a determinado contexto ou não, em comparação com a versão do framework anterior.

Outro componente necessário é a tabela de mapeamento, servindo como referência para determinar quais tipos de ameaças LINDDUN devem ser consideradas em várias combinações entre fonte, fluxo de dados e destino (Sion; Joosen, 2023) – possibilitando a indicação de ameaças já nas fases iniciais do desenvolvimento.

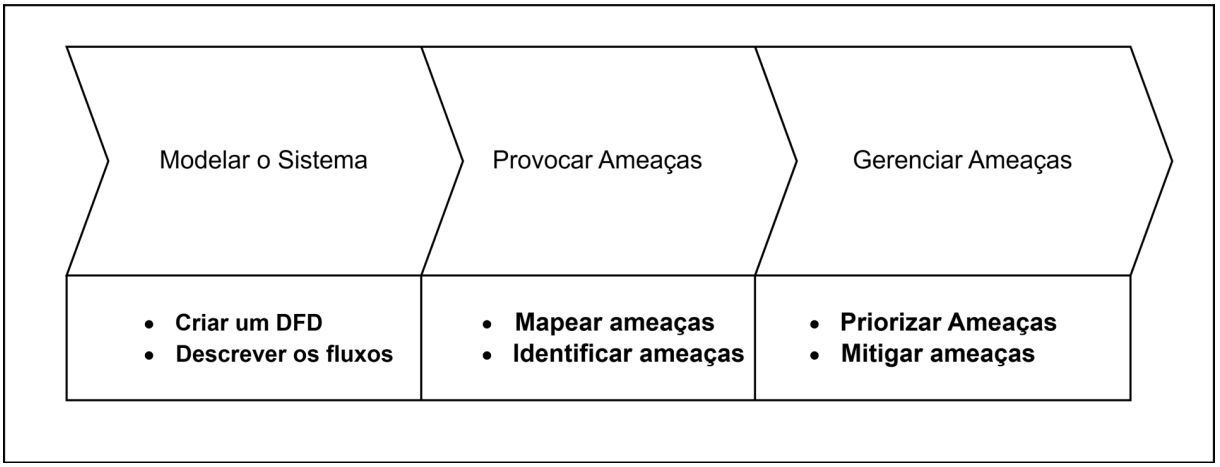
A identificação precoce dos riscos de privacidade no desenvolvimento de software ajuda a criar sistemas mais seguros desde o início, reduzindo a necessidade de correções futuras. Isso melhora a proteção da privacidade e a experiência do usuário. O software considera os critérios e ameaças das árvores de ameaças, focando nas ameaças finais identificadas na análise de privacidade.

**Etapas do Processo**

O LINDDUN PRO segue três etapas para avaliar a privacidade: modelagem do sistema, elicitação de ameaças e gerenciamento de ameaças. A primeira etapa modela o sistema com um DFD. A segunda etapa investiga ameaças e usa uma tabela de mapeamento e árvores de ameaças. A terceira etapa implementa contramedidas para mitigar ameaças e documenta tudo em um plano de ação. O processo é repetido para refletir mudanças no sistema e garantir a privacidade.

A Figura 2 representa de maneira objetiva as três etapas que devem ser executadas durante o processo de modelagem de ameaças. Sistematicamente, o processo deve ser repetido de modo que as mudanças no sistema sejam refletidas na análise de ameaças e nas contramedidas, garantindo assim a manutenção da privacidade ao longo do ciclo de vida do sistema analisado.

Figura 2 – Etapas do Processo da Modelagem de Ameaças - LINDDUN PRO




Fonte: Adaptado de INSTRUCTIONS FOR LINDDUN PRO (2024)

**Trabalhos Relacionados**

A integração da avaliação de vulnerabilidades com a segurança cibernética é progressivamente mediada pela modelagem de ameaças (Välja *et al.*, 2020). Esse processo, complexo e dinâmico, requer conhecimento técnico especializado e um investimento significativo de tempo e esforço. Torna-se necessário a adoção de ferramentas para simplificá-lo.

Uma dessas ferramentas é a Microsoft TMT (Threat Modeling Tool), um software de modelagem de ameaças bem consolidado, que possibilita o reconhecimento de ameaças classificadas pela metodologia STRIDE (Shi *et al.*, 2021) – permitindo personalizar o esquema, as ameaças e suas propriedades, e usar modelos próprios ou da comunidade.

Já a OWASP Threat Dragon (TD) é bem similar ao TMT, porém é uma ferramenta mais simples, tendo um motor de regras de ameaças identificando ameaças mais genéricas de sua metodologia principal, também a STRIDE (Shi *et al.*, 2021). Além de sua metodologia principal, o TD conta com o método LINDDUN, centrado na privacidade – no entanto, diferente do método principal, não é feita a detecção de ameaças automaticamente até o presente momento, precisando o usuário adicioná-las manualmente e individualmente.

Outro software de bastante relevância é o Threagile (TA), ágil na identificação riscos, além de empregar YAML para modelar o sistema, seus recursos, além de avaliar as ameaças com base no interesse do atacante, bem como na chance de perda de dados (Shi *et al.*, 2021).

A SPARTA é uma ferramenta que possui algumas vantagens importantes, como a detecção automática de ameaças e o foco em privacidade e segurança (Sion *et al.*, 2018). No entanto, ela também apresenta algumas limitações, como a complexidade de utilização, além do uso da metodologia antiga do LINDDUN, embora tenha sido feita uma adaptação para o novo modelo dirigido à interação (Sion *et al.*, 2018). Além de não se basear nos novos critérios de privacidade, árvores de ameaças e tabela de mapeamento definidos na nova metodologia LINDDUN PRO.

Tabela 1 – Comparação Entre as Demais Ferramentas e o Software Proposto (PTD)

| **FERRAMENTAS** | **METODOLOGIA UTILIZADA** | **SUPORTE À PRIVACIDADE?** | **DETECTA AMEAÇAS AUTOMATICAMENTE?** | **BASEIA-SE NOS CRITÉRIOS DAS ÁRVORES DE AMEAÇAS?** |
|---|---|---|---|---|
| **Threagile** | STRIDE | NÃO | SIM | NÃO |
| **Microsoft TMT** | STRIDE | NÃO | SIM | NÃO |
| **OWASP Threat Dragon** | STRIDE, LINDDUN | SIM | SIM (APENAS STRIDE) | NÃO |
| **SPARTA** | STRIDE, LINDDUN | SIM | SIM | NÃO |
| **PTD** | LINDDUN PRO | SIM | SIM | SIM |

Fonte: Autoria Própria (2024).

A Tabela 1 mostra uma comparação entre as cinco ferramentas de análise de segurança e privacidade referenciadas anteriormente – onde a primeira coluna descreve os softwares comparados: Threagile, TMT, TD, SPARTA e PTD. Já a segunda coluna retrata qual metodologia de modelagem de ameaças cada software utiliza. A terceira coluna detalha se a solução possui suporte à privacidade. E a última coluna questiona se a ferramenta se baseia nos critérios das árvores de ameaças para a análise de segurança e privacidade. Nota-se que

nenhuma das soluções citadas anteriormente satisfazem todos os requerimentos das colunas – além da proposta que este trabalho apresenta.

**Proposta: Detector de Ameaças à Privacidade**

O PTD (Privacy Threat Detector) é uma solução desenvolvida para simplificar o processo de modelagem de ameaças no contexto da privacidade, inspirado pela ferramenta Microsoft Threat Modeling Tool (TMT) que segue a metodologia STRIDE. O PTD se destaca ao adotar a metodologia LINDDUN PRO, onde é capaz de identificar até 45 vulnerabilidades com base nas árvores de ameaças associadas a esta metodologia, oferecendo uma análise detalhada das ameaças à privacidade. Além disso, uma das características importantes desta ferramenta é a presença de um motor de regras de ameaça, que se baseia não apenas nas regras fornecidas pela tabela de mapeamento, mas também nos critérios concentrados em privacidade disponibilizados nas árvores de ameaças.

Para usar a ferramenta, deve-se criar um DFD como base para a modelagem de ameaças – a opção por essa representação foi motivada por dois fatores: primeiro, os DFDs são fáceis de entender. Segundo, eles são centrados em dados, e, portanto, focam no fluxo de informações pelo sistema, que é frequentemente alvo de ataques de software (Wuyts, 2015). Posteriormente, na continuidade do uso da ferramenta, é necessário inserir respostas (sim ou não) para os critérios de privacidade das árvores de ameaças. O motor de regra de ameaças processa o DFD e os critérios para identificar ameaças à privacidade.

O motor de regras de ameaças utiliza-se das regras contidas na tabela de mapeamento, identificando e avaliando ameaças potenciais com base nos critérios dirigidos à privacidade. Ao incorporar esses critérios, o software expande as possibilidades para uma análise de ameaças adaptada aos requisitos específicos de privacidade do sistema em consideração.

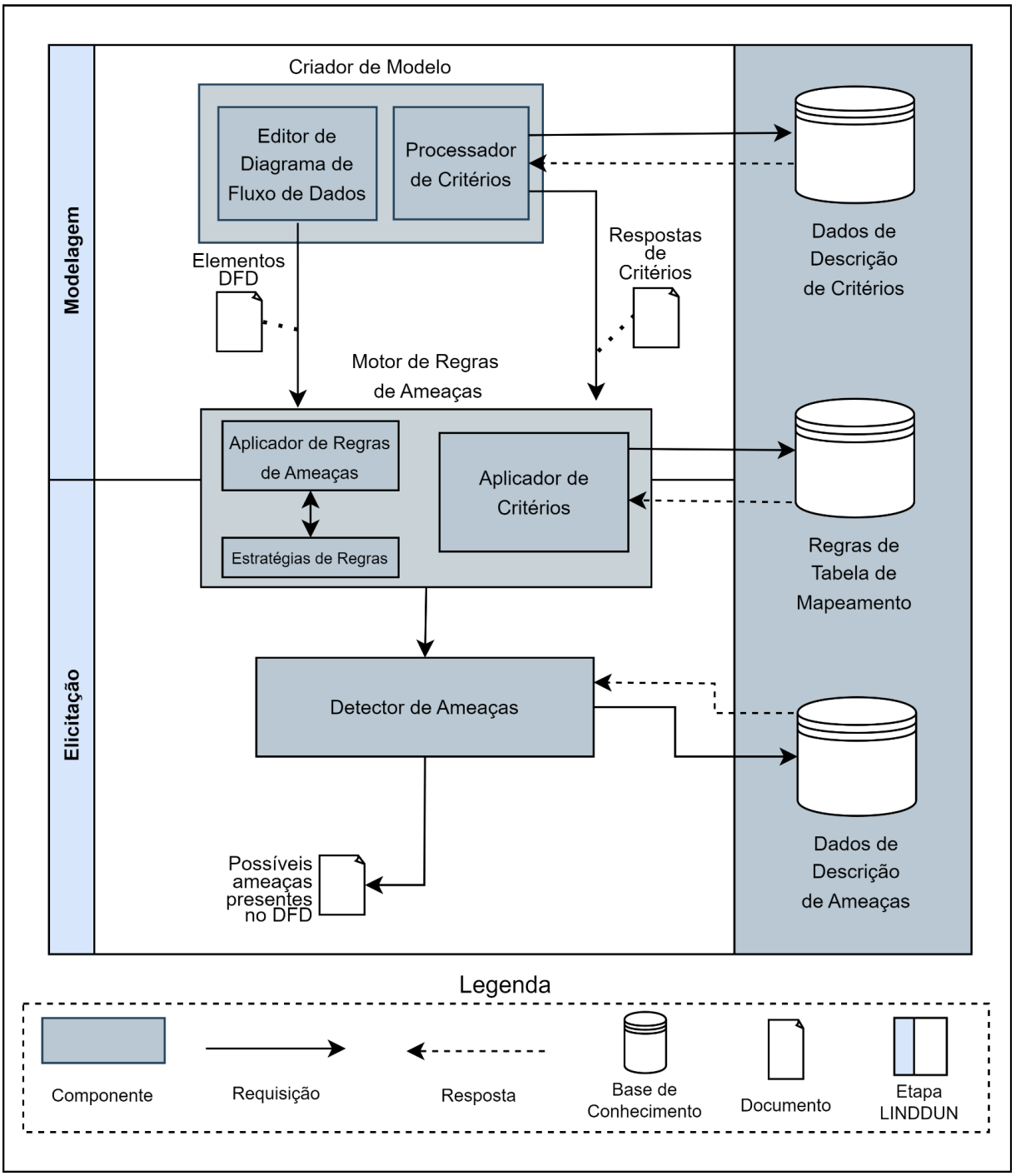
Com a ferramenta e a metodologia, profissionais de software podem identificar e abordar ameaças à privacidade. A ferramenta detecta automaticamente ameaças com base no DFD e nos critérios de privacidade, acelerando o processo.

**Arquitetura da Solução**

A ferramenta possui os componentes de criador de modelo, motor de regras de ameaças, detector de ameaças e as devidas bases de conhecimentos necessárias. A Figura 3 abaixo fornece uma visão geral da arquitetura, sendo representada por duas etapas, uma de

modelagem e outra de elicitação de ameaças – estas etapas estão diretamente ligadas ao processo de modelagem de ameaças da metodologia LINDDUN PRO.

Figura 3 – Diagrama Visão Geral da Arquitetura do Software – PTD



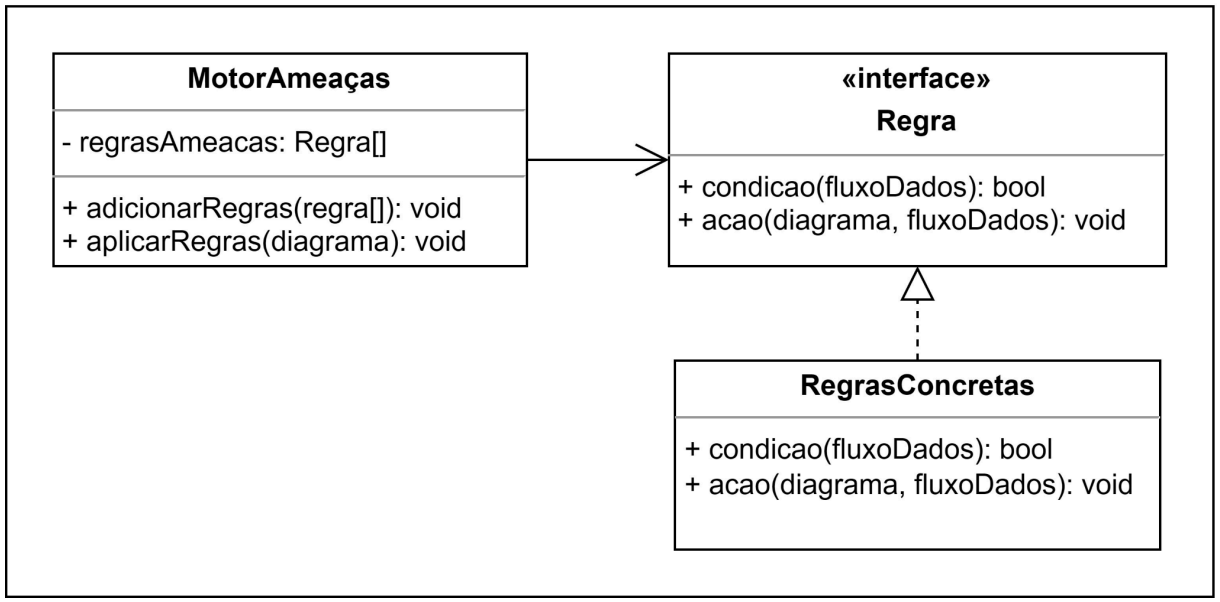

Fonte: Autoria Própria (2024).

O Criador de Modelo é um componente que facilita a modelagem e análise de riscos de sistemas baseados em fluxo de dados, utilizando a metodologia LINDDUN PRO. Ele

possui dois sub-componentes principais: o Editor de Diagrama de Fluxo de Dados e o Processador de Critérios.

O primeiro permite a representação gráfica da arquitetura do sistema, essencial para identificar pontos críticos e possíveis canais de vazamento de informação. O segundo subcomponente filtra ameaças relevantes, baseando-se nos critérios definidos pelas árvores de ameaças da metodologia. O Motor de Regras de Ameaça, por sua vez, utiliza a metodologia LINDDUN PRO para detectar ameaças de privacidade baseando-se nos fluxos de dados e regras, operando em ciclos de inferência e executando ações para cada condição que corresponde a uma ameaça de privacidade.

Figura 4 – Diagrama de Classe – Motor de Regras de Ameaças




Fonte: Autoria Própria (2024).

Com base na Figura 4, pode-se concluir que o diagrama representa um sistema que usa regras para analisar fluxos de dados. O motor de regras é responsável por aplicar as regras aos fluxos de dados. É uma abordagem na qual é empregado um conjunto de regras, onde cada regra engloba uma condição específica e uma ação correspondente (Fowler, 2010). Para um escopo que necessita um número alto de regras de negócio, essa técnica é fundamental para eficiência e organização de um sistema. Por meio desse método, as decisões e lógicas complexas podem ser definidas de maneira clara e modular, assim simplificando a manutenção e a evolução do software.

As Estratégias de Ameaças definem as propriedades das ameaças de acordo com a classe correspondente, tornando a arquitetura sustentável em termos de manutenção e escalabilidade. Isso permite a adição fácil de novas estratégias sem impactar a estrutura existente. O desacoplamento e a coesão favorecem um design robusto e compreensível, contribuindo para a resiliência do sistema diante das evoluções no cenário de privacidade.

Um pilar crucial na arquitetura são as bases de conhecimento, que representam repositórios valiosos de dados. Elas são essenciais para consultar informações relacionadas às ameaças e aos critérios focados em privacidade.

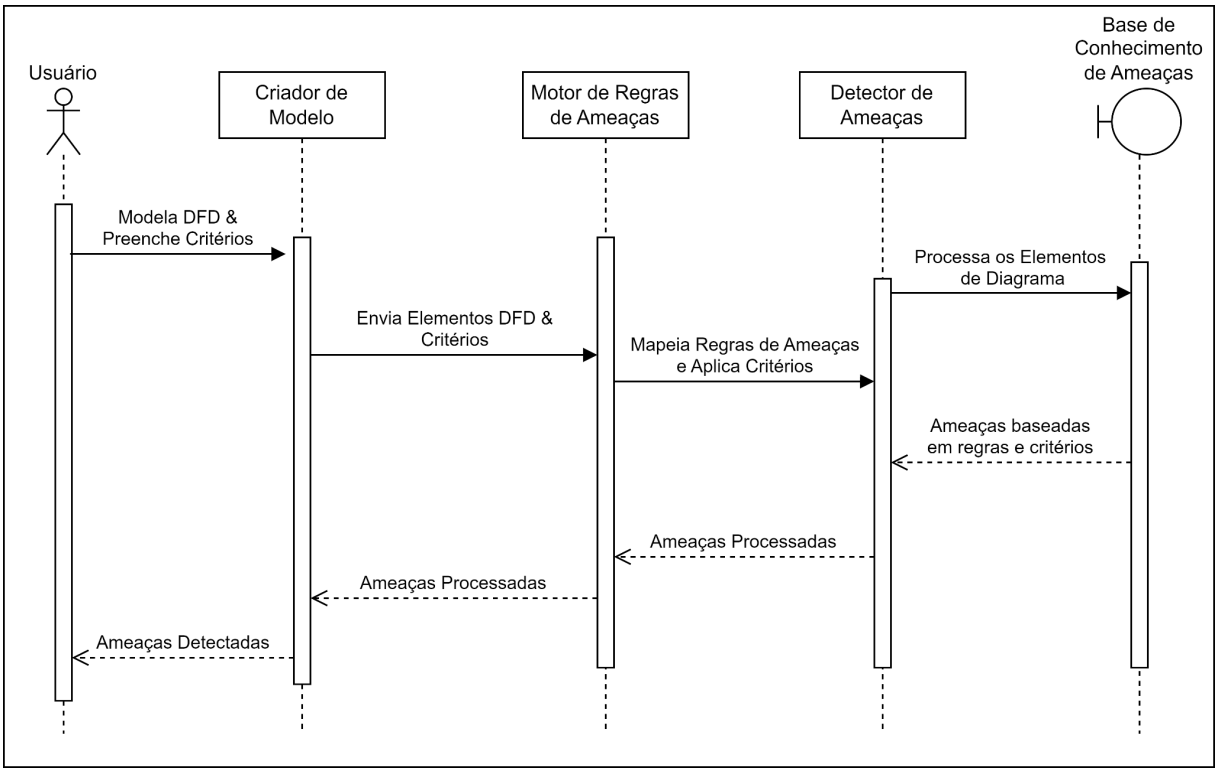
Existem três bases de conhecimento principais: Dados de Descrição de Critérios à Privacidade, Regras de Tabela de Mapeamento e Dados de Descrição de Ameaças. Dados de Descrição de Critérios à Privacidade armazena informações sobre os 59 critérios de privacidade usados para avaliar a aplicabilidade das ameaças no contexto da aplicação que está sendo modelada, seguindo as árvores de ameaças de cada categoria. Regras de Tabela de Mapeamento contém 35 regras que otimizam a detecção e análise de potenciais ameaças à privacidade, baseando-se na interação entre a origem, o fluxo de dados e o destino. Dados de Descrição de Ameaças guarda todas as informações das 45 ameaças mapeadas, incluindo título, id, exemplos, descrição e impacto. Essas bases de conhecimento desempenham um papel essencial na identificação das ameaças LINDDUN em diversas situações.

O Detector de Ameaças oferece uma representação visual clara de cada ameaça identificada. Sendo descritas com propriedades importantes, como identificação única, título elucidativo, descrição detalhada, exemplos práticos e impacto potencial no sistema. Desta forma, é possível proporcionar uma interface que permite aos usuários explorar as nuances das ameaças e sua relação com outros elementos do sistema.

**Diagrama de Sequência**

A Figura 5 mostra um diagrama de sequência que ilustra o método para identificar e processar ameaças baseadas em DFD. O método tem cinco etapas: o usuário modela o sistema alvo usando DFD e preenche critérios de privacidade. O Criador do Modelo recebe os elementos DFD e os critérios do usuário, convertendo-os em um modelo interno do sistema alvo e seus componentes.

Figura 5 – Diagrama de Sequência – Panorama Geral




Fonte: Autoria Própria (2024).

Em seguida, o modelo interno é enviado ao Motor de Regras de Ameaças, que identifica ameaças potenciais no sistema, consultando uma Base de Conhecimento de Ameaças. O Motor de Regras de Ameaças mapeia as regras de ameaças aos elementos do modelo interno e aplica as regras da tabela de mapeamento, bem como as respostas dos critérios de privacidade fornecidas pelo usuário para filtrar as ameaças relevantes. As ameaças identificadas são enviadas de volta ao usuário e ao Gerador de Ameaças, que processa essas ameaças e gera uma lista detalhada sobre elas, incluindo a descrição, a categoria e o caminho de fluxo de dados que possivelmente está comprometido.

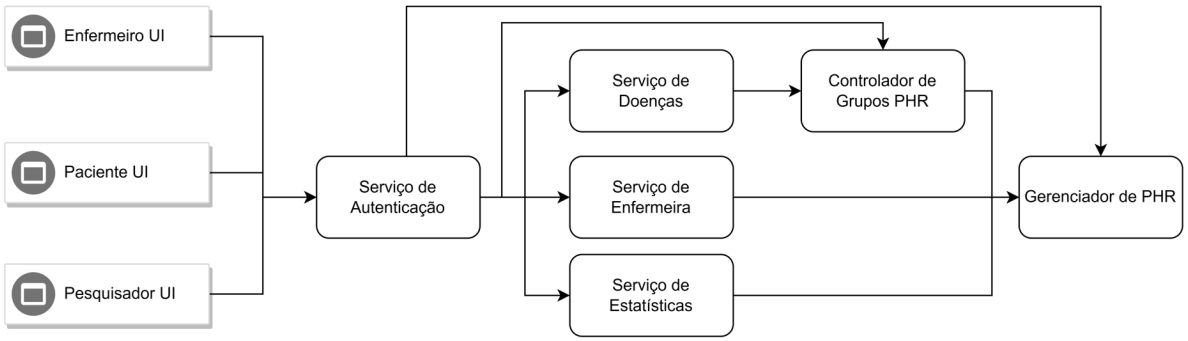
**Avaliação**

Esta seção detalha a avaliação da solução proposta em um sistema orientado a fluxo de dados. O objeto de estudo selecionado foi a plataforma Comunidades de Pacientes[3] (Kunz *et al.*, 2021), que facilita o compartilhamento de informações médicas entre pacientes com condições similares, independentemente de serem conhecidos ou não. Distinta das redes sociais convencionais, esta plataforma é centrada na saúde e bem-estar dos usuários, permitindo-lhes documentar seu histórico médico — incluindo aspectos como estado de ânimo, medicação e tratamentos — e compará-lo com o de outros usuários.

A Comunidade de Pacientes é um software complexo que simplifica a interação entre pacientes, enfermeiros(as) e pesquisadores. Ele armazena e gerencia os Registros Pessoais de Saúde (PHR) dos pacientes de forma segura, permitindo a comparação com outros usuários. Enfermeiros(as) podem adicionar novos usuários e criar grupos, facilitando o gerenciamento e a assistência. Pesquisadores podem acessar os dados PHR anonimamente, permitindo análises estatísticas e estudos — diminuindo a possibilidade de ameaças à privacidade devido aos dados serem anonimizados.

Na Figura 6, o sistema tem três interfaces de usuário (UIs) para pacientes, pesquisadores e enfermeiros, cada uma com funcionalidades exclusivas para atender às necessidades específicas de cada grupo. O backend consiste em um conjunto integrado de serviços que trabalham juntos para administrar eficientemente os PHRs, além de oferecer outros recursos essenciais.

Figura 6 – Diagrama da Arquitetura do Sistema de Comunidade de Pacientes




Fonte: Autoria Própria (2024).

[3] O repositório da aplicação está disponibilizado em: https://github.com/clouditor/patient-community-example

Entre os serviços essenciais, o mecanismo de autenticação emite tokens de segurança para acessar o sistema. O serviço de consulta de doenças permite aos pacientes pesquisar sintomas e receber uma lista inicial de diagnósticos. O controlador de grupos PHR compila os registros de saúde de todos os grupos do paciente, oferecendo uma visão completa do histórico de saúde.

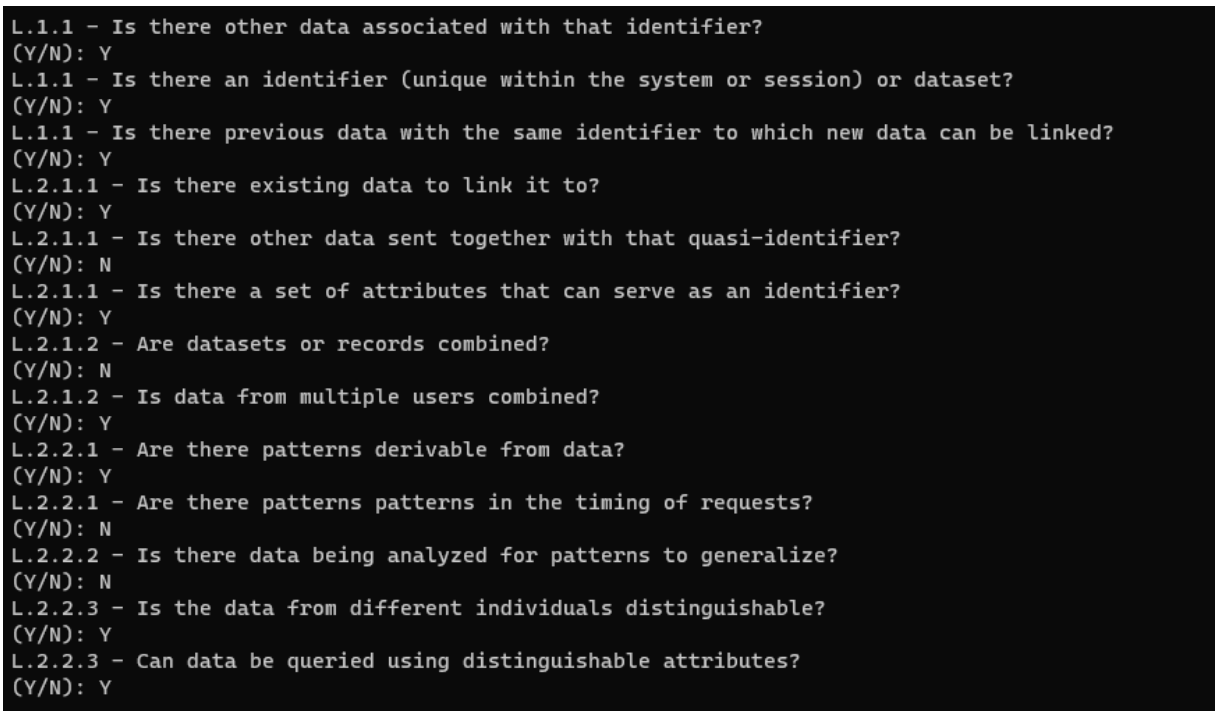
Além disso, o serviço de gestão de enfermagem supervisiona informações dos usuários, bem como atribui funções específicas a cada indivíduo no sistema. O serviço de estatísticas anonimizadas permite aos pesquisadores acessar dados estatísticos referentes aos registros de saúde sem comprometer a privacidade dos pacientes.

É importante destacar que a abordagem de avaliação visa identificar e atenuar desafios potenciais relacionados à privacidade dos dados. Dada a natureza delicada das informações de saúde, a análise é conduzida para antecipar e neutralizar qualquer vulnerabilidade que possa ameaçar a confidencialidade dos dados dos usuários.

**Utilizando a Ferramenta**

Na detecção de ameaças, é importante ter noção dos critérios a serem aplicados. Por isso, na Figura 7 é mostrado um console apresentando perguntas (critérios) respondidas com Y ou N. Se a resposta for Y, o critério é considerado para análise mais profunda pelo Motor de Regras de Ameaças. Se a resposta for N, o critério não é avaliado, poupando ameaças incompatíveis com o sistema modelado.

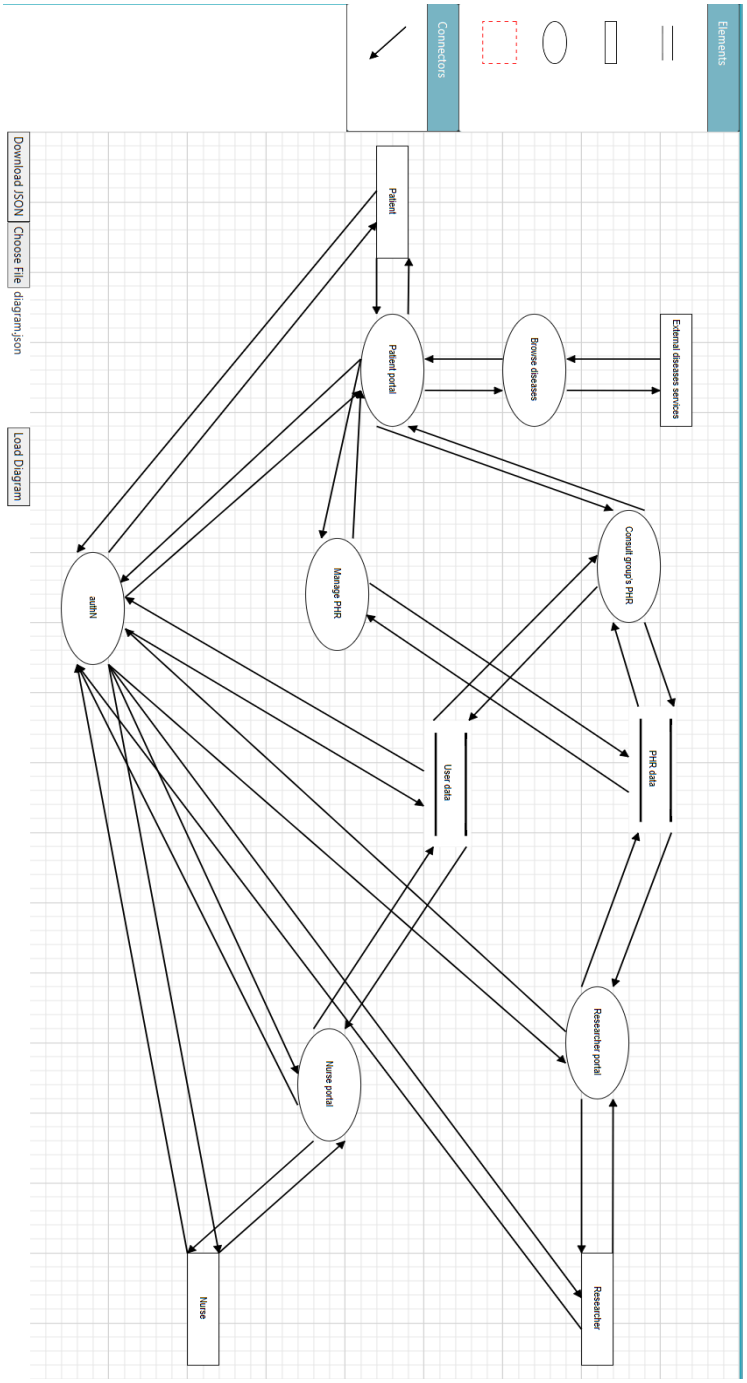
Figura 7 – Processador de Critérios de Privacidade




Fonte: Autoria Própria (2024).

A Figura 8 mostra como o software é empregado para modelar o sistema de comunidade de pacientes em um diagrama de fluxo de dados. Este processo implica a elaboração de um documento JSON, que posteriormente é submetido a uma análise. Durante essa análise, cada fluxo é cuidadosamente identificado e avaliado, garantindo sua completa validação para integração com o componente do Motor de Regras de Ameaças.

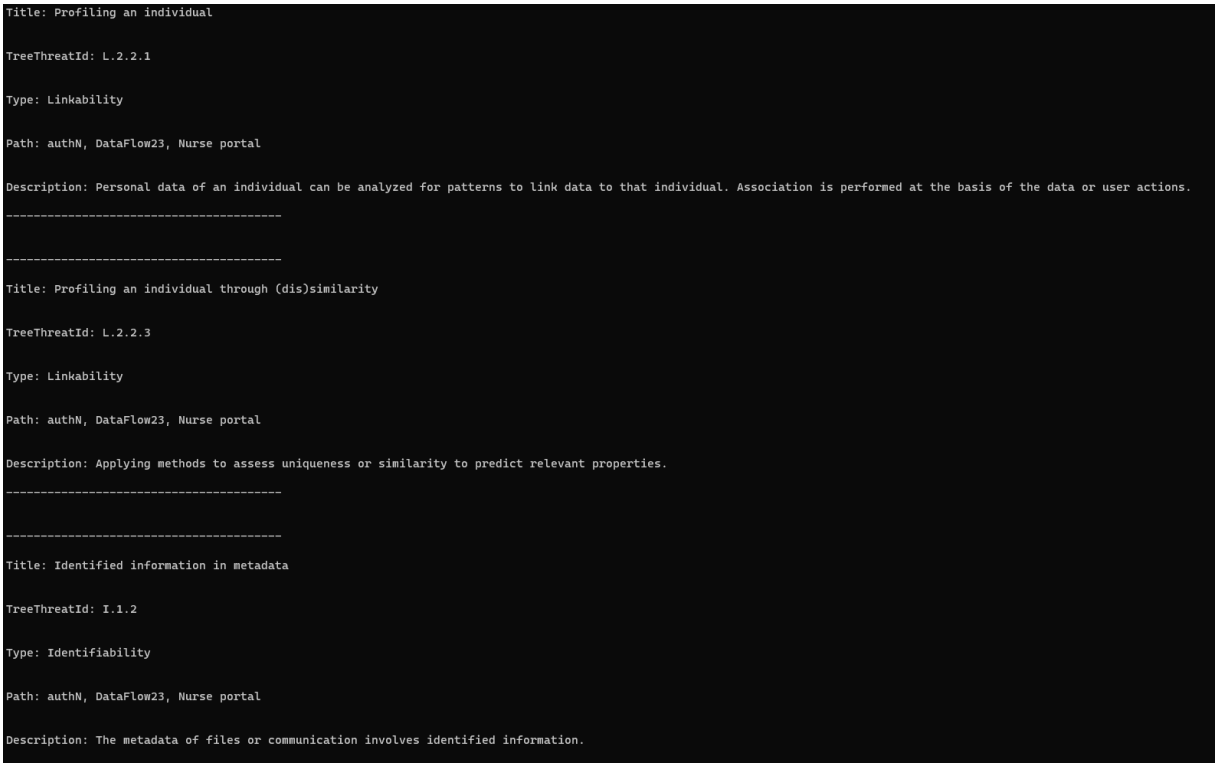
Figura 8 – Diagrama de Fluxo de Dados da Comunidade de Pacientes Usando a Ferramenta




Fonte: Autoria Própria (2024).

A Figura 9 mostra o detector de ameaças, que analisa as ameaças do sistema, e dá uma visão global da privacidade do sistema.

Figura 9 – Detector de Ameaças




Fonte: Autoria Própria (2024).

**Critérios de Privacidade Considerados**

A interpretação dos critérios de privacidade pode variar devido a informações ausentes ou não encontradas, afetando os resultados. As ameaças à privacidade são dinâmicas e evoluem ao longo do tempo, então os resultados da análise podem não ser sempre precisos. Os critérios foram baseados em informações de um documento de modelagem de ameaças[4] elaborado com a metodologia LINDDUN. (Kunz *et al.*, 2022).

As tabelas abaixo descrevem os critérios existentes para as categorias de ameaça de *Linkability, Identifiability, Non Repudiation, Detectability, Data Disclosure, Unawareness & Unintervenability* e *Non Compliance*, respectivamente. A coluna "ID AMEAÇA" informa a identificação da ameaça na árvore de ameaça relacionada com a sua categoria. Já a coluna "ID CRITÉRIO" denota um identificador para os critérios de privacidade que se repetem, pois uma ameaça pode possuir mais de um. A coluna "DESCRIÇÃO DO CRITÉRIO" mostra a pergunta que deve ser respondida no processo de detecção de ameaças. Já a coluna

[4] O documento está disponível em https://7e71aeba-b883-4889-aee9-a3064f8be401.filesusr.com/ugd/cc602e_b4f5b1fc19da49a9bb8e39f0933cadab.pdf

"JUSTIFICATIVA" representa a justificativa considerada para a resposta do critério na terceira coluna. E por fim, a última coluna expõe a aplicabilidade de cada critério.

A Tabela 2 apresenta uma análise dos critérios específicos relacionados à categoria de ameaças de *Linkability*. Esta análise ampara a avaliação da probabilidade de vinculação de dados por meio de identificadores únicos, a combinação de registros de usuários e a identificação de padrões dedutíveis nos dados. Cada critério é devidamente justificado e categorizado como aplicável ou não, proporcionando uma exposição das potenciais vulnerabilidades de linkability inerentes ao sistema em análise.

Tabela 2 – Categoria de Ameaça de *Linkability*.

| ID AMEA-ÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁVEL |
|---|---|---|---|---|
| L.1.1 | 1 | Existem outros dados associados a esse identificador? | O ID do usuário é essencial para identificar e vincular os dados de saúde de um usuário. | SIM |
| L.1.1 | 2 | Existe um identificador (único dentro do sistema ou sessão) ou conjunto de dados? | O ID do usuário é um identificador único dentro do sistema. | SIM |
| L.1.1 | 3 | Há dados anteriores com o mesmo identificador aos quais novos dados podem ser vinculados? | O ID do usuário é persistente, permitindo a vinculação de dados antigos e novos. | SIM |
| L.2.1.1 | 1 | Há dados existentes para vinculá-los? | O ID do usuário é um identificador existente que pode ser usado para vincular dados. | SIM |
| L.2.1.1 | 2 | Há outros dados enviados junto com esse quasi-identificador? | O ID do usuário é um identificador único e não é necessário enviar outros dados para ser vinculado. | NÃO |

| | | | | |
|---|---|---|---|---|
| L.2.1.1 | 3 | Existe um conjunto de atributos que pode servir como identificador? | O ID do usuário é um identificador que pode ser usado para vincular dados. | SIM |
| L.2.1.2 | 1 | Os conjuntos de dados ou registros são combinados? | Os dados de saúde são combinados pelo ID do grupo, apesar de serem armazenados separadamente. | NÃO |
| L.2.1.2 | 2 | Os dados de vários usuários são combinados? | Os dados de saúde de vários usuários podem ser combinados pelo ID do grupo. | SIM |
| L.2.2.1 | 1 | Existem padrões deriváveis dos dados? | É possível derivar padrões dos dados de saúde, como padrões de doenças ou tratamentos. | SIM |
| L.2.2.1 | 2 | Existem padrões no momento das requisições? | Os dados de saúde são anônimos, dificultando a identificação de padrões. | NÃO |
| L.2.2.2 | 1 | Os dados estão sendo analisados para generalizar padrões? | Os dados de saúde não são analisados para generalizar padrões. | NÃO |
| L.2.2.3 | 1 | Os dados de diferentes indivíduos são distinguíveis? | Os dados de saúde são anônimos, tornando difícil, mas não impossível, distinguir indivíduos. | SIM |
| L.2.2.3 | 2 | Os dados podem ser consultados usando atributos distinguíveis? | Os dados de saúde podem ser consultados usando atributos distinguíveis. | SIM |

Fonte: Autoria Própria (2024).

É verificado a presença de informações de identidade nos dados e nos metadados, o uso de identificadores únicos, o processamento de dados fornecidos pelos usuários e a coleta de dados que possam revelar identidades na Tabela 3. Com cada critério de privacidade sendo avaliado e classificado como relevante ou não de acordo com a Tabela 3.

Tabela 3 – Categoria de Ameaça de *Identifiability*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| I.1.1 | 1 | Os dados enviados para o sistema contém informações de identidade? | Os dados enviados não incluem identidade pessoal, fornecida pelos usuários. | NÃO |
| I.1.2 | 1 | Os metadados associados contêm informações identificadas? | Metadados dos dados de saúde excluem informações pessoais. | NÃO |
| I.1.2 | 2 | O sistema processa dados que têm metadados associados? | O sistema processa dados com metadados para gerenciar e fornecer insights sobre a saúde. | SIM |
| I.2.1.1 | 1 | Existe um identificador único usado em interações ou ao se referir a dados de um indivíduo? | O ID do usuário é único, gerado aleatoriamente, não derivado de dados pessoais. | SIM |
| I.2.2 | 1 | Existem dados fornecidos pelos usuários em formato livre que são recebidos ou processados pelo sistema? | O sistema não recebe dados não estruturados dos usuários. | NÃO |
| I.2.2 | 2 | São coletados dados que podem revelar informações de identificação? | O sistema coleta dados de identidade pessoais, mas os separa dos dados de saúde, dificultando a identificação. | SIM |
| I.2.3 | 1 | As solicitações ou registros são suficientemente únicos para distinguir aqueles de um indivíduo específico? | As solicitações são identificadas pelo ID do usuário, aleatório e não exclusivo. | NÃO |

Fonte: Autoria Própria (2024).

A Tabela 4 envolve a categoria de Non Repudiation, tendo o intuito de analisar o risco de um usuário negar ter realizado uma ação no sistema. Os critérios cobrem registro de dados, sensibilidade dos dados, uso de assinatura digital, presença de metadados, uso de dados ou padrões ocultos, efeitos colaterais e necessidade de negação plausível. De acordo com a Tabela 4, o sistema possui um risco moderado de negar a plausibilidade.

Tabela 4 – Categoria de Ameaça de *Non Repudiation*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| Nr.1.1 | 1 | O sistema registra dados que afetam a negação plausível? | O sistema registra dados úteis para provar ações de um usuário. | SIM |
| Nr.1.1 | 2 | Os dados em si afetam as reivindicações de negação plausível? | Dados de saúde pessoal são sensíveis e podem identificar alguém. Alterações ou exclusões podem negar ações de um usuário. | SIM |
| Nr.1.2 | 1 | Quais chaves são usadas para assinatura? Quem tem acesso a essas chaves para verificar assinaturas? | O sistema não usa assinatura digital. | NÃO |
| Nr.1.2 | 2 | Os dados são digitalmente assinados? | O sistema não usa assinatura digital. | NÃO |
| Nr.1.3 | 1 | Existem metadados associados aos dados armazenados ou transmitidos? | O modelo de dados não inclui metadados rastreáveis. | NÃO |

| | | | | |
|---|---|---|---|---|
| Nr.1.4 | 1 | Existem dados embutidos ou padrões ocultos nos dados ou transmissões? | O sistema não usa dados embutidos ou padrões ocultos. | NÃO |
| Nr.2 | 1 | As ações que requerem negação plausível têm efeitos colaterais (por exemplo, acionar, transmitir, registrar, etc.)? | Enviar um PHR a um grupo pode revelar a identidade do usuário. | SIM |
| Nr.2 | 2 | Existe uma ação que requer negação plausível de um indivíduo? | Enviar um PHR a um grupo requer negação plausível. | SIM |

Fonte: Autoria Própria (2024).

Os critérios de privacidade contidos na Tabela 5 têm o intuito de representar o risco de informações serem detectadas indevidamente. Levando em consideração observabilidade da comunicação, inferência de informações, efeitos colaterais, detecção dos efeitos, mensagens de erro e especificidade das mensagens de erro. O sistema apresenta um risco alto de detectabilidade.

Tabela 5 – Categoria de Ameaça de *Detectability*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| D.1 | 1 | A comunicação pode ser observada? | Dados pessoais são transmitidos sem criptografia, permitindo que observadores observem a comunicação. | SIM |
| D.1 | 2 | Informações podem ser inferidas das comunicações observadas? | Os dados pessoais sensíveis podem identificar indivíduos ou inferir seu estado de saúde. | SIM |

| | | | | |
|---|---|---|---|---|
| D.2 | 1 | As ações no sistema têm efeitos colaterais (por exemplo, acionar outras transmissões)? | O sistema envia informações sobre o grupo ao paciente quando este envia seu registro de saúde pessoal. | SIM |
| D.2 | 2 | Esses efeitos colaterais são detectáveis? | O sistema não indica efeitos colaterais. | NÃO |
| D.3 | 1 | O sistema mostra mensagens de erro ao recuperar dados? | É mostrado mensagens de erro ao recuperar dados. | SIM |
| D.3 | 2 | As mensagens de erro são diferentes quando o item não existe (em comparação com não ter direitos de acesso)? | As mensagens de erro são as mesmas, independentemente do motivo do erro. | NÃO |

Fonte: Autoria Própria (2024).

Neste contexto, é esclarecido a aplicabilidade dos critérios referentes às ameaças de vazamento de dados – isto é, dados não autorizados ou acidentalmente revelados, considerados como sensíveis ou confidenciais. Na Tabela 6 são levados em conta os critérios de recolhimento de dados sensíveis, detalhamento excessivo de dados, frequência pela qual os dados são processados, temporalidade na disponibilidade dos dados e acessibilidade dos dados.

Tabela 6 – Categoria de Ameaça de *Data Disclosure*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| DD.1.1 | 1 | Os dados são mais sensíveis do que estritamente necessário? | Dados pessoais são coletados e armazenados, mesmo sem necessidade. | SIM |

| | | | | |
|---|---|---|---|---|
| DD.1.2 | 1 | Os dados são mais detalhados do que estritamente necessário? | Os dados pessoais não são coletados em excesso. | NÃO |
| DD.1.3 | 1 | A codificação dos dados inclui outros (meta)dados? | Os dados pessoais são codificados com metadados identificáveis. | SIM |
| DD.2.1 | 1 | A quantidade de dados é necessária? | Há excesso na coleta de dados. | NÃO |
| DD.2.2 | 1 | A frequência de processamento é necessária? | Os dados pessoais são processados mais do que o necessário. | NÃO |
| DD.2.3 | 1 | Há mais sujeitos de dados envolvidos do que o necessário? | Os dados pessoais são coletados de mais pessoas do que o necessário. | SIM |
| DD.3.2 | 1 | Os dados são necessários para o destinatário? | Os dados pessoais são compartilhados com destinatários desnecessários. | NÃO |
| DD.3.3 | 1 | O uso de serviços (padrões) revela dados do usuário? | O uso de serviços padrão, como o JWT, pode revelar dados do usuário. | SIM |
| DD.3.4 | 1 | Os dados são armazenados por mais tempo do que o necessário? | Não há informações sobre armazenamento ou duração dos dados pessoais. | NÃO |
| DD.4.1.1 | 1 | Há mais partes envolvidas do que o necessário? | O sistema coleta e compartilha dados pessoais com partes não essenciais. | SIM |
| DD.4.1.2 | 1 | Há mais partes envolvidas do que o necessário? | O sistema coleta e compartilha dados pessoais com partes não essenciais. | SIM |
| DD.4.2 | 1 | Quão acessíveis são os dados (públicos/limitados/privados)? | Os dados pessoais são acessíveis a poucas pessoas, mas carecem de segurança adequada. | NÃO |

Fonte: Autoria Própria (2024).

A Tabela 7 tem o propósito de elucidar as ameaças relacionadas à falta de

conhecimento e consentimento. Os critérios presentes tratam-se da aplicabilidade de consentimento informado, transparência no compartilhamento de dados, controle das preferências de privacidade e configuração de como os dados pessoais são processados.

Tabela 7 – Categoria de Ameaça de *Unawareness & Unintervenability*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| U.1.1 | 1 | Os sujeitos de dados não estão suficientemente cientes de quais dados pessoais estão sendo coletados, processados, armazenados ou divulgados? | O sistema não informa aos usuários quais dados pessoais são coletados. | SIM |
| U.1.2 | 1 | Se um usuário compartilha dados pessoais de outros, fica claro o que, por que e como esses dados são posteriormente processados? | O sistema não informa se dados de terceiros serão compartilhados. | SIM |
| U.2.1 | 1 | O sujeito de dados pode alterar suas preferências posteriormente? | O sistema permite que os usuários alterem suas preferências de privacidade a posteriori. | NÃO |
| U.2.1 | 2 | O sistema permite que o sujeito de dados configure quais dados pessoais são processados e para quais fins? | O sistema utiliza dados pessoais, independente das preferências do usuário. | SIM |
| U.2.2 | 1 | Os sujeitos de dados não têm acesso aos seus dados pessoais que estão sendo coletados, processados, armazenados ou | Usuários podem ver, mudar ou apagar dados no portal. | NÃO |

| | | | | |
|---|---|---|---|---|
| | | divulgados? | | |
| U.2.3 | 1 | Os sujeitos de dados têm a capacidade de corrigir ou excluir dados pessoais? | O sistema permite que os usuários corrijam ou excluam seus dados pessoais. | SIM |

Fonte: Autoria Própria (2024).

Tabela 8 – Categoria de Ameaça de *Non Compliance*.

| ID AMEAÇA | ID CRITÉRIO | DESCRIÇÃO DO CRITÉRIO | JUSTIFICATIVA | APLICÁ-VEL |
|---|---|---|---|---|
| Nc.1.1.2 | 1 | O sistema coleta ou processa mais dados do que legalmente necessário? | Não é identificado se o sistema coleta e processa dados além do legal. | NÃO |
| Nc.1.1.3.1 | 1 | O consentimento pode ser demonstrado? | Não é fornecido informações sobre como o consentimento é coletado ou documentado. | NÃO |
| Nc.1.1.3.1 | 2 | O consentimento é livre, informado, específico e inequívoco? | Não é fornecido informações sobre como o consentimento é coletado ou documentado. | NÃO |
| Nc.1.1.3.1 | 3 | O consentimento pode ser retirado? | Não é fornecido informações sobre como o consentimento pode ser retirado. | NÃO |
| Nc.1.1.3.2 | 1 | Existem tipos especiais de processamento, como decisões automatizadas? | O sistema pode usar decisões automatizadas para recomendar grupos com base em informações de saúde. | SIM |
| Nc.1.1.3.2 | 2 | A coleta depende de bases legais válidas e apropriadas para um propósito específico? | Não é fornecido informações sobre as bases legais, de dados pessoais para decisões automatizadas. | NÃO |

| | | | | |
|---|---|---|---|---|
| Nc.1.1.4 | 1 | O sistema armazena dados por mais tempo do que legalmente necessário? | Não é fornecido informações sobre como os dados pessoais são armazenados ou por quanto tempo são armazenados. | NÃO |

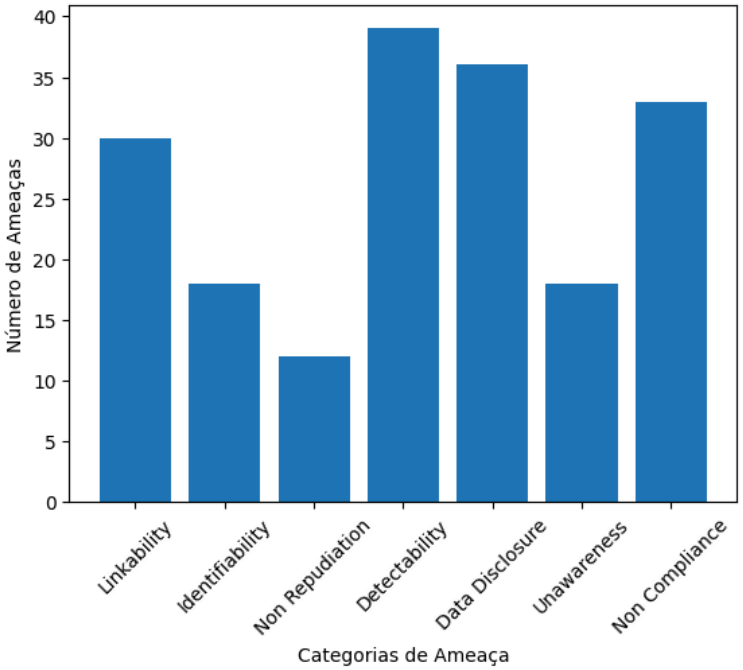
Fonte: Autoria Própria (2024).

A Tabela 8 apresenta a avaliação dos critérios de privacidade baseados na categoria de ameaça de Non Compliance. Tem a finalidade de analisar o risco de um sistema violar leis e regulamentos de proteção de dados. Ponderando sobre coleta e processamento de dados, obtenção de consentimento, retirada de consentimento, bases legais para decisões automatizadas e armazenamento de dados por tempo excessivo. O sistema apresenta um risco baixo de não conformidade com leis e regulamentos de proteção de dados - devido a não consideração de muitos critérios.

**Ameaças Encontradas**

Como resultado das entradas tanto do diagrama modelado, bem como dos critérios aplicáveis, identificamos um total de 186 possíveis ameaças. Essas ameaças foram classificadas em sete categorias, conforme apresentado no gráfico a seguir.

Figura 10 – Gráfico de Ameaças Encontradas na Avaliação




Fonte: Autoria Própria (2024).

O gráfico da representado na Figura 10 revela que as categorias *Detectability*, *Data Disclosure* e *Non Compliance* são as mais prevalentes, com 39, 36 e 33 ameaças identificadas, respectivamente. Isso indica um risco significativo de violação da privacidade, seja por não conformidade de leis ou regulamentos, divulgação inadequada de dados ou dificuldade de identificar e responder a violações de privacidade. As categorias de *Linkability*, *Identifiability* e *Unawareness* são as quartas, quintas e sextas mais prevalentes, com 30, 18 e 18 ameaças respectivamente. Isso significa que há um risco, tal que os dados pessoais dos usuários sejam não só vinculados uns aos outros, como também da identidade dos usuários seja revelada, além do desconhecimento do uso de alguns dados. Por fim, a categoria de não repúdio representa 12 ameaças.

Esse panorama destaca a complexidade das ameaças à privacidade na aplicação do Sistema de Comunidade de Pacientes e reforça a importância de uma abordagem contínua na pesquisa, buscando explorar diferentes perspectivas para uma compreensão mais abrangente das ameaças em potencial. Isto é, as informações podem ser usadas para orientar o desenvolvimento quanto às medidas de mitigação e para melhorar a conscientização dos usuários sobre os riscos de privacidade associados ao uso do sistema.

## Considerações Finais

Neste trabalho, desenvolvemos uma ferramenta que possibilita modelar diagramas de fluxo de dados e detectar ameaças à privacidade de forma semi-automatizada baseada na metodologia de modelagem de ameaças LINDDUN PRO. O propósito desta aplicação consiste em empregar critérios e regras de forma a reduzir substancialmente a necessidade de detectar ameaças manualmente.

Os resultados obtidos neste trabalho demonstram que a ferramenta proposta é uma contribuição relevante para o campo da modelagem de ameaças à privacidade, pois oferece uma forma mais ágil em realizar essa atividade, baseando-se em critérios e regras – o que pode representar uma abordagem inovadora ou uma melhoria significativa em relação às ferramentas existentes. A ferramenta pode ser útil para os desenvolvedores de software que buscam aprimorar a proteção da privacidade em seus sistemas, bem como para os pesquisadores que desejam explorar novas abordagens e técnicas para a modelagem de ameaças.

Além disso, o trabalho apresenta algumas limitações que se configuram como oportunidades para pesquisas futuras. Não foi avaliada a precisão das ameaças detectadas – se eram falsos positivos ou falsos negativos. Também não foi considerado premissas específicas do sistema analisado. Outro fator relevante para o trabalho seria a recomendação de mitigações automáticas para cada ameaça detectada. A possibilidade de geração de artefatos como relatório contendo gráficos, poderiam facilitar a compreensão das ameaças. Além do mais, sugestões para pesquisas futuras incluem a exploração do uso de inteligência artificial na modelagem de ameaças aplicada à privacidade. E por fim, uma possível metodologia de modelagem de ameaças à privacidade focada na LGPD (Lei Geral de Proteção de Dados).

## Referências


ALSHAMMARI, M.; SIMPSON, A. C. Towards a Principled Approach for Engineering Privacy by Design. **Annual Privacy Forum**, 2017.

SPIEKERMANN, Sarah. The challenges of privacy by design. **Communications of the ACM 55**, 38-40, 2012.

MCGRAW, G. **Software Security: Building Security In**. Addison-Wesley Professional, Boston, 2006.

SOUPPAYA, M.; SCARFONE, K. Guide to Data-Centric System Threat Modeling. **NIST**, 800-154, 2016. Disponível em: <https://csrc.nist.gov/pubs/sp/800/154/ipd>. Acesso em: 16 ago. 2023.

KUNZ, I. et al. Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-based Analysis. **Proceedings on Privacy Enhancing Technologies**, 2023.

TORR, P. Demystifying the Threat-Modeling Process. **IEEE Security and Privacy Magazine**, v. 3, n. 5, p. 66–70, set. 2005.

HERNAN, S.; LAMBERT, S.; OSTWALD, T.; SHOSTACK, A. Uncover Security Design Flaws Using The STRIDE Approach. **MSDN Magazine**, 2016. Disponível em: <https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach>. Acesso em: 17 ago. 2023

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, 16 nov. 2010.

SELIN, J. **Evaluation of Threat Modeling Methodologies: A Case Study**. 2019. Tese (Mestrado em Cyber Segurança) – JAMK University of Applied Sciences, Jyväskylä, 2019.

SHOSTACK, A. **Threat Modeling: Designing for Security**. Wiley, Indianapolis, 2014.

DEMARCO, T. **Structured Analysis and System Specification**. Yourdon Press, New York, 1981.

WUYTS, K. **Privacy Threats in Software Architectures**. 2015. Tese (Doutorado em Engenharia) – Katholieke Universiteit Leuven, Flandres, 2015.

SION, L. **Automated Threat Analysis for Security and Privacy**. 2020. Tese (Doutorado em Engenharia) – Katholieke Universiteit Leuven, Flandres, 2015.

SION, L. et al. Solution-aware data flow diagrams for security threat modeling. **Proceedings of the 33rd Annual ACM Symposium on Applied Computing**, 9 abr. 2018.

SION, L. et al. SPARTA: Security & Privacy Architecture Through Risk-Driven Threat Assessment. **2018 IEEE International Conference on Software Architecture Companion (ICSA-C)**, abr. 2018.

GALVEZ, R.; GURSES, S. The odyssey: Modeling privacy threats in a brave new world. **2018 IEEE European Symposium on Security and Privacy Workshops**, abr. 2018.

KERAMATI, H.; MIRIAN-HOSSEINABADI, S.-H. Integrating software development security activities with agile methodologies. **2008 IEEE/ACS International Conference on Computer Systems and Applications**, abr. 2018.

SION, L; JOOSEN, W. **LINDDUN PRO Privacy Threat Modeling Tutorial**. Technical Report, Department of Computer Science, Katholieke Universiteit Leuven, abr. 2023.

FOWLER, M. **Domain-Specific Languages**, Addison-Wesley Professional, Boston, 2010.

MICHAEL, J. Privacy and Human Rights: An International and Comparative Study, With Special Reference to Developments in Information Technology. **UNESCO**, Paris, 1994.

CAVOUKIAN, A. **Privacy by Design: The 7 Foundational Principles**. Information and Privacy Commissioner of Ontario, Canada, 2009.

YSKOUT, K. et al. Threat modeling: from infancy to maturity. **2020 IEEE/ACM 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)**, 2020.

SCANDARIATO, R.; WUYTS, K.; JOOSEN, W. A descriptive study of Microsoft's threat modeling technique. **Requirements Engineering**, v. 20, n. 2, p. 163–180, 3 dez. 2013.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 15 dez. 1890.

ROTENBERG, M. Protecting Human Dignity in the Digital Age. **2000 International Congress on Infoethics 2000: Ethical, Legal and Societal Challenges of Cyberspace**, 3rd, Paris, 2000.

BERTINO, E. Data Security and Privacy: Concepts, Approaches, and Research Directions. **2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)**, 2016.

ALAFAA, P. Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World. **SSRN Electronic Journal**, 2022.

VÄLJA, M. et al. Automating threat modeling using an ontology framework. **Cybersecurity**, v. 3, n. 1, 1 out. 2020.

**INSTRUCTIONS FOR LINDDUN PRO** (2024). Disponível em: <https://linddun.org/instructions-for-pro>. Acesso em: 2 de jan. 2024.

**LINDDUN PRO** (2024). Disponível em: <https://linddun.org/pro>. Acesso em: 21 de fev. 2024.

KUNZ, I. et al. **Patient Community – A Test Bed for Privacy Threat Analysis**. 2021. Disponível em: <https://github.com/clouditor/patient-community-example>. Acesso em: 30 dez. 2023.

TUMA, K. et al. Towards Security Threats that Matter. Lecture Notes in Computer Science, p. 47–62, 22 dez. 2017.

SHI, Z. et al. Threat Modeling Tools: A Taxonomy. **IEEE Security & Privacy**, p. 2–13, 2021.

SION, L. et al. Interaction-Based Privacy Threat Elicitation. Lirias (KU Leuven), 1 abr. 2018.

XIONG, Wenjun; LAGERSTRÖM, Robert. Threat modeling – A systematic literature review. **Computers & Security**, [s. l.], v. 84, p. 53–69, 2019.