Universidade Federal do Amazonas
Instituto de Computação
Programa de Pós-Graduação em Informática

Andrey Antonio de Oliveira Rodrigues

PTMOL - Uma Linguagem para Modelagem de Ameaças de Privacidade orientada a Redes Sociais Online

Manaus
Março de 2023

Andrey Antonio de Oliveira Rodrigues

PTMOL - Uma Linguagem para Modelagem de Ameaças de Privacidade orientada a Redes Sociais Online

Tese de Doutorado submetida ao Programa de Pós-Graduação em Informática da Universidade Federal do Amazonas.

Orientador: Prof. Dr. Eduardo Luzeiro Feitosa

Coorientadora: Prof. Dra. Maria Lúcia Bento Villela

Manaus
Março de 2023

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

R696p

Rodrigues, Andrey Antonio de Oliveira
PTMOL - Uma linguagem para modelagem de ameaças de privacidade orientada a redes sociais online / Andrey Antonio de Oliveira Rodrigues . 2023
195 f.: il. color; 31 cm.

Orientador: Eduardo Luzeiro Feitosa
Coorientadora: Maria Lúcia Bento Villela
Tese (Doutorado em Informática) - Universidade Federal do Amazonas.

1. Modelagem de ameaças. 2. Privacidade. 3. Design de privacidade. 4. Redes Sociais Online. 5. Estudos empíricos. I. Feitosa, Eduardo Luzeiro. II. Universidade Federal do Amazonas III. Título

FOLHA DE APROVAÇÃO

"PTMOL - Uma Linguagem para Modelagem de Ameaças de Privacidade orientada a Redes Sociais Online"

Andrey Antônio de Oliveira Rodrigues

Tese de Doutorado defendida e aprovada pela banca examinadora constituída pelos Professores:

Prof. Dr. Eduardo Luzeiro Feitosa - PRESIDENTE

Prof. Dr. Raimundo da Silva Barreto - MEMBRO INTERNO

Documento assinado digitalmente
gov.br
CRISTIANO MACIEL
Data: 14/03/2023 19:58:26-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Cristiano Maciel - MEMBRO EXTERNO

Documento assinado digitalmente
gov.br
ANA CAROLINA ORAN ROCHA
Data: 14/03/2023 12:21:38-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Ana Carolina Oran Rocha - MEMBRO EXTERNO

Documento assinado digitalmente
gov.br
CAROLINE QUEIROZ SANTOS
Data: 14/03/2023 15:53:24-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Caroline Queiroz Santos - MEMBRO EXTERNO

Manaus, 09 de Março de 2023

Agradecimentos

Agradeço, em primeiro lugar, a Deus, que tem iluminado meu caminho durante esta jornada, concedendo-me luz, força e sabedoria para que eu conseguisse seguir até aqui. Tenho certeza que sem Ele nada disso seria possível.

Agradeço, imensamente, a minha mãe e a minha avó que, de forma especial e carinhosa, me deram força e coragem, apoiando todas as minhas decisões. Chegar até aqui não seria possível sem o o incentivo e impulso que elas sempre me emitiram. Em todos os momentos de dificuldades pensava nelas e no quanto eu queria que elas sentissem orgulho de mim.

Agradeço ao meu orientador, professor Eduardo Feitosa, que vem me auxiliando em todos os momentos desta caminhada, por estar sempre disposto a colaborar. Por ser, além de tudo, um excelente orientador, que sempre me concedeu incentivos durante as orientações e por sempre acreditar em mim e confiar no meu trabalho. Obrigado, professor, pela paciência e amizade.

Agradeço a minha coorientadora, Maria Lúcia, a quem admiro não só por colaborar com o meu trabalho, mas pela pessoa maravilhosa e generosa que sempre foi. Muito obrigado pelo apoio constante, pelo voto de confiança e amizade. Agradeço por sempre me mostrar o caminho certo, me incentivar e, acima de tudo, por aumentar meu conhecimento. Espero seguir seu exemplo e ser um grande profissional como você.

Agradeço aos membros da banca por aceitarem o convite para participar da defesa da minha tese. Escolhemos vocês porque os enxergamos como grandes referências e exemplos a serem seguidos.

Obrigado a minha família e aos meus grandes amigos que torceram muito por mim, me passando as melhores vibrações e energias positivas.

À CAPES, pelo apoio financeiro. À UFAM, ao IComp, por prover a infraestrutura.

Por fim, também agradeço a todos que participaram dos estudos conduzidos neste trabalho, pela colaboração, paciência e contribuições.

"*Alguns homens veem as coisas como são e dizem 'Por quê?' Eu sonho com as coisas que nunca foram e digo 'Por que não?'*"

(George Bernard Shaw).

Resumo

As Redes Sociais Online (RSOs) tornaram-se um dos principais fenômenos tecnológicos da Web, ganhando uma popularidade eminente entre seus usuários. Com a crescente expansão mundial dos serviços de RSOs, as pessoas passaram a dedicar tempo e esforço para manter e manipular sua identidade online nesses sistemas. Contudo, o processamento de dados pessoais por meio dessas redes tem exposto os usuários a diversos tipos de ameaças de privacidade. Consequentemente, novas soluções necessitam ser desenvolvidas para o tratamento dos cenários de ameaças aos quais um usuário está potencialmente exposto. Neste sentido, este trabalho propõe a PTMOL *(Privacy Threat Modeling Language*), uma linguagem de apoio à modelagem de ameaças de privacidade orientada à RSOs. Por meio de um mapeamento sistemático da literatura, foi possível identificar e analisar as principais lacunas não cobertas pelas soluções vigentes. A partir desse mapeamento, foi possível desenvolver uma nova solução, a qual foi refinada e adaptada para o contexto de privacidade em RSOs. A linguagem proposta visa apoiar a busca antecipada por ameaças às quais um usuário poderá está exposto e quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. A linguagem foi avaliada por meio da condução de um conjunto de estudos empíricos que permitiram realizar os procedimentos de validade e confiabilidade da proposta. Os resultados dos estudos indicam que o emprego da linguagem é potencialmente útil para a identificação de ameaças reais de privacidade devido ao caráter exploratório e reflexivo da mesma. Portanto, a PTMOL pode ser incorporada ao desenvolvimento de RSOs durante o nível de design e pode auxiliar projetistas e engenheiros de software a introduzir modelagem de ameaças em seus projetos, sem exigir um alto nível de especialidade na área de privacidade.

Palavras-chave: Modelagem de ameaças, privacidade, design de privacidade, redes sociais online, estudos empíricos.

Abstract

Online Social Networks (OSNs) have become one of the main technological phenomena on the Web, gaining eminent popularity among its users. With the growing worldwide expansion of OSN services, people have begun to dedicate time and effort to maintaining and manipulating their online identity in these systems. However, the processing of personal data through these networks has exposed users to various types of privacy threats. Consequently, new solutions need to be developed to deal with the threat scenarios to which a user is potentially exposed. In this sense, this work proposes PTMOL *(Privacy Threat Modeling Language*), a language for modeling privacy threats in OSNs. Through a systematic mapping of the literature, it was possible to identify and analyze the main gaps not covered by the current solutions. From this mapping, it was possible to develop a new solution, which was refined and adapted to the context of privacy in OSNs. The proposed language aims to support the early search for threats to which a user may be exposed and what privacy controls an OSN needs to define to reduce the effects and consequences of these threats. The language was evaluated by conducting a set of empirical studies that allowed carrying out the proposal's validity and reliability procedures. The results of the studies indicate that the use of language is potentially useful for identifying real threats to privacy due to its exploratory and reflective nature. Therefore, PTMOL can be incorporated into the development of OSNs during the design level and can help designers and software engineers to introduce threat modeling into their projects, without requiring a high level of expertise in the area of privacy.

Keywords: Threat modeling, privacy, privacy by design, online social network, empirical study.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

Este capítulo apresenta a introdução a esta tese de doutorado. Além de contextualizar esta pesquisa, são apresentados: a definição do problema, os objetivos, a metodologia, as principais contribuições e a organização do trabalho.

1.1 Contexto

As Redes Sociais Online (RSOs) tornaram-se um dos principais fenômenos tecnológicos da Web, ganhando uma popularidade eminente entre seus usuários. Em geral, uma RSO pode ser definida como uma rede de interações e relacionamentos (Aggarwal, 2011). Uma definição mais clássica apresenta as RSOs como sistemas baseados na Web, que oferecem aos usuários a possibilidade de construir um perfil público ou semipúblico e estabelecer uma conexão virtual entre pessoas com interesses, gostos e atividades em comum (Boyd and Ellison, 2007). Sites de RSOs, como Facebook e Twitter, incentivam e fomentam esse processo por meio de recursos que permitem que seus usuários compartilhem informações com públicos grandes e diversos.

Atualmente, as RSOs fornecem diversas funcionalidades e serviços que atraem cada vez mais usuários. Por exemplo, permitem analisar dados e correlacionar as preferências dos usuários para fornecer serviços avançados e personalizados. Com isso, podem recomendar amigos ou interesses em comum com base nas informações extraídas dos perfis e atividades dos usuários, como preferências, navegação diária, entre outros (Oukemeni et al., 2019). Além disso, as mudanças sociais e os movimentos políticos acrescentaram um novo papel para esses sistemas. As RSOs tornaram-se fonte de cobertura jornalística e meio de propagação de diversos tipos de informação, como o movimento "Primavera Árabe", no Oriente Médio e Norte da África (Khondker, 2011), e os "Motins de Londres" (Panagiotopoulos et al., 2014).

Com a popularidade mundial dos serviços de RSOs, as pessoas passaram a dedicar tempo e esforço para manter e manipular sua identidade online nesses sistemas. À medida que os usuários confiam cada vez mais nessas aplicações para suas atividades de comunicação, o processamento de dados pessoais por meio dessas redes tem exposto os

usuários a diversos tipos de ameaças de privacidade (Rathore et al., 2017; Siddula et al., 2018; Ali et al., 2018). Uma ameaça de privacidade é um evento indesejável potencial ou real que pode causar divulgação, exposição e uso indevido de dados privados do usuário (Joyee De and Imine, 2019; Laorden et al., 2010). Sua consequência é a violação de privacidade, onde dados pessoais são divulgados a indivíduos ou entidades não autorizados, para fins maliciosos (Abawajy et al., 2016b). O incidente no Facebook - Cambridge Analytica é um exemplo proeminente de violação, onde dados pessoais de um grande número de usuários foram divulgados e a maioria desses indivíduos não tinha controle nem conhecimento dessa divulgação (Solon, 2018).

A coleta e o processamento de dados por meio das RSOs nem sempre são transparentes ou controláveis pelos usuários. Geralmente, ao aceitar fazer parte de uma determinada RSO, os usuários dão seu pleno consentimento aos provedores, por meio dos termos de uso, para armazenar e analisar seus dados e, às vezes, vendê-los a terceiros para fins de publicidade e marketing (Oukemeni et al., 2019). Além disso, os provedores de serviços também controlam os bancos de dados onde as informações dos usuários são armazenadas. Nesse sentido, o elevado número de dados pessoais compartilhados nesses sistemas torna os usuários alvos desejáveis para atacantes. Um atacante é o agente da ameaça que tem como objetivo coletar e utilizar as informações pessoais de um usuário da RSO para atividades indevidas ou maliciosas (Wang and Nepali, 2015). Um atacante pode encontrar facilmente informações relevantes de usuários, como sua identidade ou localização. De posse desses dados, ele pode cometer diversos crimes, como fraudes ou roubo de identidade (Rathore et al., 2017).

Algumas RSOs, como o Twitter, por exemplo, fornecem aos seus usuários um espaço para interações curtas e rápidas. Com isso, as postagens acabam sendo dinâmicas e seu conteúdo não contém muitas informações privadas significativas. No entanto, atacantes podem analisar essas informações curtas para tentar inferir outras informações não divulgadas (Song et al., 2014). Estudos apontam que os atributos privados da personalidade de um usuário podem ser inferidos com base nas suas "curtidas" em postagens de RSOs (Kosinski et al., 2013; Briola et al., 2018). Esses julgamentos baseados em "curtidas" podem ser ainda mais precisos do que aqueles feitos por amigos e parentes próximos do usuário (Youyou et al., 2015).

Com o aumento expressivo do número de ameaças de privacidade devido ao compartilhamento de dados pessoais em RSOs, muitos pesquisadores propuseram diferentes abordagens para preservar a privacidade, o anonimato e a confidencialidade dos usuários (Zeng et al., 2015; Abid et al., 2018b; Wen et al., 2018; Al-Asmari and Saleh, 2019a). Entretanto, essas abordagens, no geral, são direcionadas para mitigar ameaças e vulnerabilidades e reduzir os riscos relacionados ao funcionamento e arquitetura desses sistemas. Assim, ainda que mecanismos sejam implementados para que os usuários possam configurar a visibilidade das suas publicações e limitar o acesso ao seus perfis e conteúdos, alguns desses controles permanecem insuficientes para proteger os usuários contra ameaças de privacidade. Isto pode estar relacionado ao fato de que ainda existem lacunas no design de prevenção de ameaças de privacidade em RSOs, com foco no usuário.

Nesse sentido, uma estratégia para tratar as questões mencionadas é antecipar a preocupação com a privacidade para as etapas que antecedem o desenvolvimento de aplicações sociais. Essa estratégia promissora em relação à privacidade é conhecida como privacidade desde o design (*Privacy by Design*) (Cavoukian et al., 2009). O conceito foi introduzido por uma especialista em privacidade, Ann Cavoukian. A ideia central é incorporar a privacidade e a proteção de dados pessoais nos estágios iniciais do ciclo de desenvolvimento de sistemas, em vez de tratá-los em momentos posteriores.

Na área de Interação Humano-Computador (IHC), diferentes técnicas apoiam o design de sistemas, tais como a criação de personas, modelagem de tarefas, modelagem de interação e construção de *mockups* (Barbosa and Silva, 2010). Entretanto, essas propostas generalistas não possuem características específicas para tratar ameaças de privacidade em tempo de design. Técnicas tradicionais de segurança previamente estabelecidas podem oferecer suporte à antecipação da preocupação com ameaças nos estágios iniciais do desenvolvimento de sistemas. Uma técnica amplamente usada nesse contexto é a modelagem de ameaças.

A modelagem de ameaças foi inicialmente introduzida pela Microsoft (Microsoft, 2003). A proposta foi apresentada para ser incorporada na etapa de design de segurança, visando tornar as aplicações desenvolvidas pela companhia mais seguras (Shostack, 2008). Em linhas gerais, a modelagem de ameaças visa propor uma metodologia sistemática e estruturada para identificar potenciais ameaças e vulnerabilidades para reduzir o risco aos recursos de um sistema. Ela também ajuda profissionais de TI a entenderem o impacto das ameaças, quantificar sua gravidade e implementar contramedidas. É uma atividade essencial para descobrir as armadilhas potenciais de um atacante para um sistema. No contexto da segurança, é uma técnica bem conhecida e usada por especialistas para descobrir ameaças, sendo considerada um dos pilares na construção de um sistema seguro (Shostack, 2014; Xiong and Lagerström, 2019).

A modelagem de ameaças também apresenta uma metodologia proativa para descobrir ameaças geralmente não consideradas ou encontradas por meio de revisões de código e outros tipos de auditoria (Xiong and Lagerström, 2019). Com isso, permite que uma equipe de projeto possa determinar contramedidas eficazes para combater as ameaças desde o início. Tal procedimento tende a ser cada vez mais demandado por diversas empresas, principalmente por conta da adequação com as leis gerais de proteção de dados.

1.2 Definição do Problema

Conforme apresentado, nota-se que existe uma ampla importância em antecipar a preocupação com ameaças desde os estágios iniciais do desenvolvimento de uma RSO. Embora existam propostas de modelagem de ameaças para determinados domínios (UcedaVelez and Morana, 2015; Potteiger et al., 2016; Wuyts et al., 2018), muitas dessas foram desenvolvidas para tratar ameaças de segurança e reduzir os riscos relacionados ao funcionamento e arquitetura de sistemas gerais e possuem características que dificultam sua aplicação, ou não são suficientes, para uma modelagem de ameaças com foco na

privacidade do usuário. Uma solução não deve somente atender aos requisitos funcionais e ajudar a resolver os problemas do sistema, mas deve também focar no usuário, o principal alvo da violação de privacidade. Desta forma, torna-se necessário propor novas soluções que visem tratar essa lacuna, pois, até o presente momento, não foram identificadas propostas de modelagem de ameaças com foco central na privacidade do usuário e que permita sua utilização no design de RSOs.

A identificação de ameaças de privacidade por meio de uma abordagem de modelagem pode promover os seguintes benefícios: (i) a antecipação, ainda em fase de design, dos cenários de ameaças aos quais um usuário poderá estar potencialmente exposto; (ii) a priorização dos esforços de privacidade; (iii) a justificativa para tomada de decisões informadas sobre o risco de privacidade do usuário; (iv) maior assertividade na implantação de mecanismos de privacidade, uma vez que as ameaças identificadas partem de uma visão diretamente ligada ao usuário, sob a ação de um potencial atacante; e (v) o apoio a profissionais com pouca experiência em privacidade, ajudando-os a introduzir privacidade no início do ciclo de desenvolvimento de RSOs.

Nesse contexto, esta pesquisa é motivada pelo desenvolvimento de uma solução que possibilite identificar ameaças potenciais de privacidade em RSOs, suas consequências e como elas podem ser mitigadas, visando antecipar a preocupação com a proteção dos dados do usuário desde o design. Com base nisso, a questão de pesquisa deste trabalho é: *"É possível proteger a privacidade de usuários de RSOs utilizando modelagem de ameaças?"*.

Priorizar as questões de privacidade nas etapas que antecedem o desenvolvimento de RSOs pode auxiliar o designer a refletir sobre as principais ameaças que um usuário pode enfrentar ao compartilhar suas informações pessoais nesses sistemas. Também pode auxiliar uma equipe de projeto a pensar em diretrizes úteis que ajudem a prevenir os riscos associados às ameaças. Além disso, a modelagem de ameaças tende a ser cada vez mais demandada, pois seu resultado pode melhorar a confiança dos usuários nos sistemas e garantir a conformidade com as leis gerais para proteção de dados pessoais. Portanto, diagnosticar e resolver as ameaças que um usuário está exposto é um passo importante no sentido de permitir um melhor design da próxima geração de RSOs.

1.3 Objetivos

O objetivo principal desta pesquisa consiste em propor uma linguagem de modelagem de ameaças de privacidade em RSOs, com foco em apoiar a proteção de dados do usuário durante o design de RSOs. Para atingir esse propósito geral, buscou-se dividi-lo nos seguintes objetivos específicos:

- Identificar as ameaças mais críticas para a privacidade do usuário no domínio de RSOs, com a finalidade de caracterizar o estado da arte, e empregá-las na linguagem proposta.
- Definir elementos para compor uma notação adequada para a modelagem de ameaças de privacidade ao contexto de RSOs, com foco na proteção do usuário.

- Avaliar o uso da linguagem por meio de evidências empíricas.

O objetivo final é apresentar uma linguagem de apoio a modelagem de ameaças de privacidade em RSOs, que pode ser aplicada em nível de design. Espera-se, com isso, contribuir para apoiar designers na tomada de decisões mais preventivas sobre ameaças de privacidade, ajudando-os a introduzir privacidade no início do ciclo de desenvolvimento de aplicações sociais.

1.4 Metodologia de Pesquisa

A metodologia da pesquisa representa o caminho do pensamento a ser seguido, tratando, basicamente, dos métodos a serem adotados para construir um conhecimento. Este processo de construção de conhecimento deve envolver o uso de estudos para testar modelos e hipóteses, assegurando que o entendimento atual do campo é correto (Minayo, 1994; Mendes, 2005). Desta forma, torna-se relevante a utilização de estratégias empíricas para testar se o que se está propondo é válido. Com isso, avaliações empíricas devem ser executadas e repetidas para testar a viabilidade da proposta, proporcionando assim uma melhor compreensão e análise sobre a construção do conhecimento (Shull et al., 2001).

A metodologia utilizada nesta pesquisa tem como fundamentação o ciclo de *Design Science Research* (DSR) (Wieringa, 2014). O DSR é um paradigma que estabelece as etapas de uma pesquisa para resolver um problema por meio da criação de um artefato, avaliando o que foi projetado e comunicando os resultados obtidos no contexto da pesquisa. A saída do DSR pode ser constructos, modelos, métodos, instanciações e melhores teorias.

O ciclo de DSR inicia com a investigação de um problema. Em seguida são especificados artefatos como soluções, os quais são avaliados para o contexto da pesquisa. Se os resultados da solução não produzirem os efeitos desejados, pode-se dar início a uma nova volta no ciclo de DSR. O processo metodológico adotado é ilustrado na Figura 1.1. As atividades executadas em cada etapa serão descritas resumidamente a seguir:

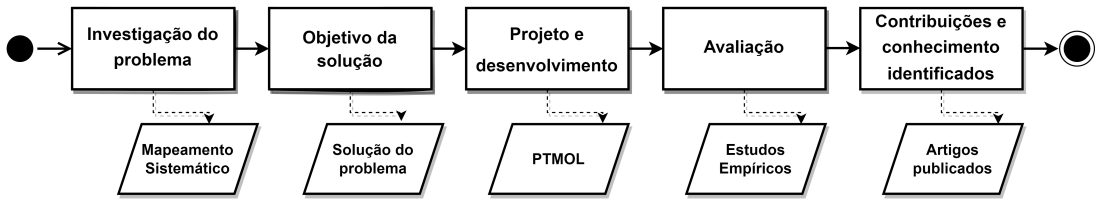


Figura 1.1: Visão ilustrativa da metodologia baseada no ciclo de DSR
Fonte: Adaptado de Lacerda et al. (2013)

- **Investigação do problema**: Essa etapa tem como objetivo investigar e compreender o problema que o pesquisador deseja estudar e solucionar, identificando

as soluções vigentes. Uma investigação foi conduzida, possibilitando analisar as características de propostas já existentes e extrair elementos necessários para a proposição de uma nova solução. Essa etapa foi realizada por meio da atividade descrita abaixo:

  - Mapeamento Sistemático da Literatura (MSL): um protocolo para a condução de um MSL foi elaborado e executado, objetivando compreender o estado da arte sobre as principais ameaças de privacidade específicas para o contexto de RSOs e soluções para mitigá-las. Foram consideradas tanto as soluções generalistas quanto as soluções que utilizam modelagem de ameaças. Os resultados do MSL permitiram identificar evidências sobre as ameaças mais críticas para a privacidade do usuário, bem como identificar as lacunas não cobertas pelas soluções existentes.

- **Objetivo da solução:** Nessa etapa, o pesquisador sugere possíveis soluções para o problema que está sendo estudado, ou seja, qual artefato deseja desenvolver. O pesquisador utiliza sua criatividade e seus conhecimentos prévios para propor soluções que possam ser utilizadas para a melhoria da situação atual. Com isso, foi definida uma solução inicial conforme descrita abaixo.

  - Solução inicial: foram obtidos *insights* para o planejamento e adequação de uma solução que promovesse a preocupação com ameaças de privacidade desde os estágios iniciais do desenvolvimento de uma aplicação social. Esses *insights* foram obtidos com base nos resultados do MSL realizado na etapa anterior e por meio da análise das principais lacunas encontradas nas soluções existentes. A solução identificada foi a modelagem de ameaças.

- **Projeto e desenvolvimento:** Nesta etapa, o pesquisador utiliza o conhecimento teórico existente para propor artefatos como solução do problema. Com base no planejamento realizado na etapa anterior, observou-se a necessidade de uma solução que permitisse representar a modelagem de ameaças com foco na privacidade do usuário. Dessa forma, foram definidos os elementos para a nova solução, bem como a sua proposta inicial, descritos abaixo:

  - Definição dos elementos: Uma análise sobre os elementos que integravam a metodologia de modelagem de ameaça foi realizada em termos de adequação ao contexto de privacidade em RSOs. Para tal, os elementos foram alvos de três decisões estratégicas: exclusão do elemento, adaptação do elemento e inserção de um novo elemento. Elementos excluídos foram aqueles considerados não aplicáveis ao domínio de RSOs. Os elementos adaptados foram aqueles que necessitaram de modificações para serem incluídos na modelagem de ameaças de privacidade orientada a RSOs. Por fim, os elementos inseridos foram aqueles que não pertenciam à modelagem de ameaças tradicional e foram incluídos na nova solução.

  - Proposta da linguagem PTMOL: com base nos elementos previamente definidos, uma nova solução para modelagem de ameaças de privacidade em RSOs foi elaborada. A solução foi denominada PTMOL (*Privacy Threat MOdeling Language*).

- **Avaliação e refinamento da solução:** Nesta etapa, o pesquisador avalia o uso do artefato para solucionar o problema abordado na pesquisa, explorando os seus efeitos no ambiente real do problema. O pesquisador deve contrastar os resultados obtidos com os objetivos da solução definidos na segunda etapa do DSR. Caso o resultado encontrado não seja o esperado, poderá retornar à etapa de projeto e desenvolvimento, a fim de desenvolver um novo artefato. Para avaliar e refinar a solução proposta, foram conduzidos estudos empíricos, conforme descritos a seguir:

  - Estudo preliminar para validação da linguagem: um estudo preliminar foi conduzido com o propósito de fortalecer os procedimentos de validade e confiabilidade da linguagem proposta, bem como identificar oportunidades de melhorias. Além disso, essa etapa também possibilitou agregar qualidade à linguagem e, sobretudo, analisar sua aplicação em tempo de uso.
  - Estudo de viabilidade: foi conduzido com o propósito de verificar a viabilidade de uso da PTMOL e se ela atendia aos objetivos gerais estabelecidos. Além disso, o estudo também foi executado para coletar oportunidades de refinamento para a PTMOL, bem como testar hipóteses sobre a sua utilização.
  - Estudo de observação: para investigar e compreender de forma aprofundada o processo de aplicação da PTMOL. Por meio desse estudo, foi possível identificar percepções e comportamentos sobre o uso dos elementos da PTMOL.
  - Estudo com especialistas: foi realizado com propósito de examinar a confiabilidade dos resultados produzidos pelo processo de modelagem proposto pela PTMOL. Com isso, o estudo foi realizado objetivando comparar os resultados produzidos com a modelagem PTMOL em relação a uma identificação *ad hoc* de ameaças.

- **Contribuições e conhecimento identificados:** Nesta etapa, o pesquisador apresenta o problema que foi estudado e sua importância, a qual pode ser realizada por meio de publicações acadêmicas.

Nota-se que a metodologia de DSR não está preocupada exclusivamente com o entendimento do problema, mas sim com as suas possíveis soluções. Nesse sentido, a metodologia tem um processo que busca operacionalizar as pesquisas que têm como objetivo projetar ou desenvolver um artefato, ou, ainda, prescrever uma solução. Embora ela seja orientada à solução de problemas, ela não busca a solução ótima, mas sim a solução satisfatória para os problemas que estão sendo estudados. Além disso, embora o problema endereçado seja único e específico, as soluções que são obtidas a partir

da condução da DSR devem ser passíveis de generalização para uma certa classe de problemas (Dresch et al., 2015).

1.5 Principais Contribuições

A principal contribuição desta pesquisa consiste na proposta da PTMOL, uma linguagem de apoio a modelagem de ameaças de privacidade em RSOs, no nível de design. Esta linguagem foi desenvolvida a partir de evidências coletadas na literatura e foi avaliada empiricamente por meio de um conjunto de estudos. Uma das principais contribuições da proposta apresentada nesta tese é busca antecipada por ameaças às quais um usuário poderá está exposto e quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. Além disso, a linguagem pode ser incorporada ao desenvolvimento de RSOs durante a fase de design e pode auxiliar designers e engenheiros de software a introduzir modelagem de ameaças em seus projetos, sem exigir um alto nível de especialidade na área de privacidade.

1.6 Organização do Texto

Esta tese de doutorado está organizada em 6 capítulos, incluindo este introdutório, que apresentou a contextualização, a definição do problema, os objetivos e a metodologia de pesquisa referente ao trabalho. O restante do trabalho está estruturado conforme descrito a seguir:

- **Capítulo 2 – Fundamentação Teórica**: expõe a base teórica na qual a elaboração da PTMOL como um todo está fundamentada. Apresenta também os trabalhos relacionados com o tema da pesquisa.
- **Capítulo 3 – Mapeamento Sistemático da Literatura**: apresenta o mapeamento sistemático realizado com o propósito de identificar e caracterizar as ameaças de privacidade mais críticas em RSOs e soluções vigentes para tratá-las. Apresenta também os principais *gaps* não cobertos pelas soluções existentes.
- **Capítulo 4 - PTMOL - *Privacy Threat MOdeling Language***: apresenta a linguagem proposta para apoiar a modelagem de ameaças de privacidade em RSOs com foco na proteção de dados do usuário, destacando seu vocabulário, sintaxe e semântica, bem como todos os seus recursos de aplicação.
- **Capítulo 5 - Avaliação e Evolução da PTMOL por meio de Estudos Empíricos**: apresenta avaliações da PTMOL por meio de estudos empíricos, onde são apresentados e discutidos resultados quantitativos e qualitativos da linguagem e refinamentos.
- **Capítulo 6 - Conclusões e Perspectivas Futuras**: apresenta as conclusões da pesquisa consolidando seu propósito e suas contribuições, e apontando algumas direções de oportunidades de trabalhos futuros.

Capítulo 2

Fundamentação Teórica e Trabalhos Relacionados

Este capítulo apresenta a contextualização bibliográfica acerca do fenômeno de interesse deste trabalho, onde são abordados os conceitos sobre privacidade e suas principais propriedades, ameaças e violações de privacidade e modelagem de ameaças. Também são apresentados os principais trabalhos relacionados com o tema da pesquisa.

2.1 Introdução

O uso expressivo de RSOs deu origem a um grande volume de dados compartilhados pelo usuário, a maioria dos quais são gratuitos e disponibilizados publicamente (Oukemeni et al., 2019). Grande parte desse conteúdo consiste em informações de caráter pessoal, cuja disponibilidade online pode representar um sério risco para a privacidade, anonimato e confidencialidade do usuário (Rathore et al., 2017; Ali et al., 2018).

Existem algumas perguntas importantes a serem respondidas para compreender o que são ameaças de privacidade no contexto de RSOs. Primeiramente, o que é privacidade em RSOs? Em seguida, o que é uma ameaça de privacidade? Por último, mas não menos importante, o que é uma violação de privacidade? A seguir, será apresentado, exemplificado e relacionado os conceitos envolvidos na fundamentação teórica deste trabalho, que inspiraram reflexões relevantes para a modelagem de ameaças de privacidade nesses sistemas.

2.2 Privacidade

De acordo com a teoria da regulação da privacidade apresentada por Altman (1975), a privacidade é definida como a capacidade do indivíduo controlar quais informações são divulgadas, para quem, quando e sob quais circunstâncias. Nessa teoria, a privacidade foi concebida como um processo de regulação de limites, no qual os indiví-

duos controlam a quantidade de informações sobre si próprio, que podem ser divulgadas a outras pessoas. Portanto, a privacidade é o direito do indivíduo controlar suas informações pessoais, saber ou restringir como elas são coletadas, transferidas, armazenadas e utilizadas.

Com base na teoria de Altman (1975), manter níveis adequados de divulgação de informações pessoais em um ambiente de comunicação e interação social é essencial para preservar a privacidade. No entanto, controlar níveis de divulgação de dados em RSOs pode ser difícil, devido às características peculiares dessas aplicações, tais como compartilhamento em massa de conteúdo e transmissão de informações (Derlega and Chaikin, 1977; Petronio, 2002).

Nesse sentido, a privacidade depende também do contexto do conteúdo compartilhado. Nissenbaum (2004) enfatiza que a privacidade só pode ser compreendida considerando-se um contexto específico, ou seja, não existem normas universais para abordá-la. Assim, a noção de privacidade é diferente para cada situação ou contexto. Ela também considera que os limites de acesso apontados por Altman (1975) são regidos por um conjunto de normas relacionadas e dependentes do contexto, como a adequação social e o fluxo de informação. A norma de adequação social determina que tipo de informação pessoal é apropriada para compartilhar em uma determinada situação ou ambiente social. As normas de fluxo de informação, por sua vez, ajudam a definir as relações pelo tipo de informação compartilhada entre as pessoas, ou seja, as pessoas compartilham informações mais pessoais com amigos mais íntimos e informações mais gerais com pessoas que não conhecem.

2.2.1 Ameaça de Privacidade

Os perfis dos usuários de RSOs, bem como o rastreamento de suas atividades online, podem revelar diversas informações significativas e privadas sobre eles. Isso se deve à disposição dos usuários em aumentar suas interações dentro desses sistemas, mas também ao pouco conhecimento sobre ameaças para a privacidade. Uma ameaça de privacidade é um evento indesejável potencial ou real que pode causar divulgação, exposição ou uso indevido de dados privados do usuário (Joyee De and Imine, 2019; Laorden et al., 2010). As ameaças podem ocorrer em aplicações que não são necessariamente maliciosas, mas que coletam ou armazenam informações pessoais mais do que o necessário. As ameaças de privacidade podem surgir dentro ou fora do sistema, de usuários próprios da rede ou de usuários maliciosos, que se disfarçam de usuários legítimos do sistema ou encontram maneiras de contornar os controles de privacidade.

Em aplicações como as RSOs, o compartilhamento de informações e dados pessoais pode ser o foco desejável para atacantes. A divulgação de localização, por exemplo, pode resultar em ameaças de rastreamento, que buscam analisar o comportamento geral dos usuários (Xu et al., 2005). Além disso, um atacante também pode coletar informações para obter pistas sobre diversos dados privados do usuário, como estilo de vida, horário e finalidade dos movimentos em diferentes locais. Um atacante também poderá receber atualizações da localização do usuário em tempo real, que podem ser usadas para identificar as suas rotas frequentemente percorridas. (Gonzalez et al., 2014).

2.2.2 Violação de Segurança vs. Violação de Privacidade

Muito embora a segurança e a privacidade tenham o mesmo propósito, que é a proteção de dados pessoais, ambas possuem abordagens bastante distintas para alcançar seu objetivo principal. Para melhor compreender a diferença entre as áreas, usamos a definição de violação de segurança e violação de privacidade para contrastá-las.

A violação de segurança refere-se ao acesso não autorizado a dados privados que estão protegidos por mecanismos de segurança; enquanto que a violação de privacidade refere-se à descoberta e divulgação direta ou indireta de informações privadas que estão disponíveis publicamente, com ou sem conhecimento prévio do usuário (Vu et al., 2019). Em outras palavras, a segurança está focada em proteger os dados contra abuso e acesso não autorizado e eventuais ataques cibernéticos. Já a privacidade está preocupada em proteger a forma como os dados são coletados, compartilhados e utilizados. A importância da privacidade dos dados está sendo cada vez mais reconhecida como um desafio para as RSOs, como evidenciado pelo vazamento de dados pessoais envolvendo milhões de usuários do Facebook – Cambridge Analytica (Solon, 2018).

No geral, uma violação de privacidade é uma consequência da execução de uma ameaça, gerando divulgação e exposição indevida dos dados do usuário, o que pode causar assédio, perda financeira e até roubo de identidade. Uma violação também pode tornar os usuários vulneráveis a usos maliciosos como golpes e crimes, que podem prejudicar sua reputação social ou situação econômica e torná-los vítimas de chantagem ou violência física (Shokri et al., 2012). Além disso, entidades comerciais e governamentais também podem violar a privacidade dos usuários para diferentes fins, como marketing direcionado, triagem de saúde ou monitoramento político (Zheleva and Getoor, 2009).

2.2.3 Propriedades de Privacidade

Para ter um aporte teórico sobre propriedades desejáveis de privacidade que tratam ameaças no contexto de RSOs, estudou-se detalhadamente as definições de propriedades de privacidade. O conjunto de propriedades apresentados nesta seção foram extraídos da terminologia proposta por Pfitzmann and Hansen (2010), pois é amplamente reconhecida na comunidade de pesquisa de privacidade, e também das definições da Organização Internacional para Padronização (ISO). São elas (Pfitzmann and Hansen, 2010; Rannenberg, 2011; Wuyts et al., 2014):

- **Desvinculação**. Refere-se a capacidade de ocultar o vínculo (relação) entre duas ou mais ações, identidades ou informações do usuário. O agente malicioso não pode ser capaz de identificar se dois itens estão relacionados.

- **Anonimato e Pseudonimato**. O atacante não pode ser capaz de identificar um indivíduo dentro de um conjunto de indivíduos anônimos. Um pseudonimato é um identificador de um indivíduo diferente de um dos seus nomes reais.

- **Negação plausível**. Refere-se à capacidade de negar ter realizado uma ação que outras partes não podem confirmar nem contradizer. Em outras palavras, um

agente malicioso não pode provar que um usuário sabe, fez ou disse algo. Por exemplo, caso o usuário faça uma denúncia, eles vão querer negar ter enviado uma determinada mensagem para proteger sua privacidade.

- **Não detecção**. Refere-se a ocultação das atividades do usuário. Por exemplo, um atacante não pode ter a capacidade de distinguir de forma precisa se alguém ou ninguém está em um determinado local.
- **Confidencialidade**. Refere-se a ocultação dos conteúdos dos dados do usuário ou liberação controlada desses conteúdos. No geral, a confidencialidade significa preservar as restrições de acesso e divulgação de informações. Embora a confidencialidade seja considerada uma propriedade de segurança, ela também é importante para preservar propriedades de privacidade, como anonimato e desvinculação. Portanto, a confidencialidade também é considerada um importante objetivo de privacidade.
- **Conscientização**. Com o surgimento das RSOs, os usuários tendem a fornecer um grande volume de informações aos provedores de serviços e perdem o controle sobre seus dados pessoais. Assim, a propriedade de conscientização tem o propósito de garantir que os usuários têm conhecimento sobre a coleta do seus dados pessoais e que apenas as informações necessárias devem ser utilizadas para permitir o desempenho da funcionalidade dos sistemas.
- **Conformidade e Transparência**. Exige que todo o sistema que armazena dados do usuário informe o titular dos dados sobre a política de privacidade do sistema e permita que o titular dos dados especifique consentimentos em conformidade com a legislação, antes que os usuários acessem o sistema.

2.3 Modelagem de Ameaças

A modelagem de ameaças foi inicialmente proposta para identificar e priorizar ameaças de segurança e determinar contramedidas para prevenir ou mitigar os efeitos dessas ameaças (Shostack, 2014). A metodologia permite que desenvolvedores, designers e analistas de sistemas possam incorporar a modelagem de ameaças no ciclo de desenvolvimento de software. Além disso, a metodologia permite gerar um modelo de ameaças e determinar quais mitigações são necessárias durante um estágio inicial do desenvolvimento de um novo sistema, aplicativo ou recurso. Portanto, modelar e avaliar ameaças potenciais durante a fase de design é um passo essencial para economizar recursos significativos que podem ser necessários para um (re)projeto (UcedaVelez and Morana, 2015; Xiong and Lagerström, 2019).

Sendo um dos principais objetivos da modelagem de ameaças fornecer diretrizes úteis sobre como mitigar os riscos associados às ameaças, torna-se necessário compreender os elementos correspondentes ao processo, os quais são integrados a um Ciclo de Risco (CR), conforme mostrado na Figura 2.1 (Laorden et al., 2010).

Figura 2.1: Ciclo de Risco da Modelagem de Ameaças
Fonte: Adaptado de Laorden et al. (2010)

O CR é composto por ativos que são comprometidos por ameaças; ameaças que exploram vulnerabilidades, que quando mal utilizadas expõe um recurso do sistema a um risco potencial. Finalmente, as contramedidas mitigam os perigos causados por esses riscos; contramedidas que têm como objetivo proteger os ativos. A seguir, são fornecidas definições para esses termos encontrados em diversos trabalhos de modelagem de ameaças na área de segurança (Laorden et al., 2010; Xiong and Lagerström, 2019; Shi et al., 2021), mas que podem ser aplicados à modelagem de ameaças de privacidade:

- **Ativo**: entidade de valor para o negócio ou empreendimento, seja processador de computador, disco, link de rede, programa, dado ou usuário.
- **Ameaça**: qualquer circunstância ou evento com potencial para causar danos a um sistema na forma de destruição, divulgação, modificação de dados e/ou negação de serviço.
- **Vulnerabilidade**: fraqueza na segurança do sistema que pode ser explorada para violar a política de segurança do sistema; a possibilidade de uma exploração ou exposição a uma ameaça, específica para uma determinada plataforma.
- **Risco:** expectativa de perda expressa como a probabilidade de uma determinada ameaça explorar uma determinada vulnerabilidade com um determinado resultado prejudicial.
- **Contramedida:** qualquer ação, dispositivo, procedimento, técnica ou outra medida que reduza a vulnerabilidade ou ameaça a um sistema.

- **Ataque:** o ato de tentar burlar os controles de segurança de um sistema. O grau de sucesso depende da vulnerabilidade do sistema ou atividade e da eficácia das contramedidas existentes.

No geral, o ciclo de risco apresentado acima endereça elementos importantes para modelagem de ameaças mas com o foco central na segurança do sistema. Tais elementos podem ser utilizadas como base para a proposição de soluções focada na privacidade do usuário. Nesse sentido, uma análise sobre esses termos adotados pela metodologia de modelagem de ameaças de segurança foi realizada para serem integrados a uma nova solução de modelagem de ameaças com o foco em privacidade. Essa análise é apresentada em detalhes no capítulo 4. A seguir serão apresentados os principais trabalhos relacionados com esta pesquisa.

2.4 Trabalhos Relacionados

Nesta seção, serão apresentados os principais trabalhos relacionados, os quais foram utilizados para a compreensão do estado da arte do tema de fundo e para identificação das principais lacunas que esta pesquisa de doutorado busca solucionar. Para um melhor entendimento, esta seção foi dividida em três subseções: a subseção 2.4.1 discorre sobre o contexto geral de modelagem de ameaças, apresentando as principais metodologias propostas para outros contextos que não são de RSOs. Já a subseção 2.4.2 apresenta o contexto atual de modelagem de ameaças no cenário de RSOs. Por fim, a subseção 2.4.3 apresenta técnicas auxiliares envolvidas no processo de modelagem de ameaças.

2.4.1 Propostas Generalistas para Modelagem de Ameaças

Na década de 90, Loren Kohnfelder e Praerit Garg propuseram a metodologia STRIDE, que inclui o gerenciamento sistemático de várias ameaças de segurança desde o estágio de design de todos os produtos da Microsoft (Khan et al., 2017). O acrônimo STRIDE é formado pelas iniciais das seguintes categorias de ameaças: *spoofing, tampering, repudiation, information disclosure, denial of service* e *elevation of privilege*. Atualmente, o STRIDE é o método de modelagem de ameaças mais refinado e utilizado no contexto do design de segurança (Kim et al., 2021).

O processo geral de modelagem de ameaças com a metodologia STRIDE engloba 6 passos: (i) identificar ativos, (ii) criar uma arquitetura geral da aplicação, (iii) decompor a aplicação, (iv) identificar as ameaças, (v) documentar as ameaças e (vi) classificar as ameaças (Kim et al., 2021). A saída desse processo gera um modelo de ameaça composto pela visão arquitetural do sistema e uma lista de ameaças associadas à aplicação de forma categorizada e classificada por severidade.

Em síntese, a primeira etapa dessa metodologia visa identificar os ativos do sistema que se deseja proteger. Esses ativos podem ser, por exemplo, páginas Web, o servidor de banco de dados da aplicação, entre outros. A partir da identificação dos ativos, a metodologia propõe a criação de uma arquitetura geral do sistema. A fase de

decomposição busca uma visão mais aprofundada sobre o sistema por meio do uso de um DFD (diagrama de fluxo de dados), que ajuda a visualizar as funcionalidades e a comunicação entre os componentes do sistema. Um DFD usa quatro símbolos padrão: (i) entidade externa; (ii) armazenamento de dados; (iii) processo e (iv) fluxo de dados. Na fase de identificação de ameaças, deve-se utilizar o esquema de categorização de ameaças STRIDE e associá-lo a cada componente do DFD, conforme mostrado na Tabela 2.1. Posteriormente, na fase de documentação de ameaças, o STRIDE fornece um documento destinado ao registro das ameaças identificadas. Por fim, a última etapa recomenda usar um modelo de avaliação de risco para classificar as ameaças por severidade.

Tabela 2.1: Elementos de um diagrama de fluxo de dados associados as ameaças STRIDE

Elementos do DFD	**S**	**T**	**R**	**I**	**D**	**E**
Entidade externa	X		X			
Processo	X	X	X	X	X	X
Fluxo de Dados		X		X	X	
Armazenamento de Dados		X		X	X	

Na mesma direção, Wuyts et al. (2018) desenvolveram uma metodologia para a modelagem de ameaças com foco em privacidade. Essa solução fornece suporte estruturado para guiar analistas e arquitetos de software na elicitação e mitigação de ameaças em sistemas gerais. Assim como o STRIDE, o nome do método é um acrônimo, que significa que as categorias de ameaças são codificadas no nome LINDDUN *(Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance)*. A metodologia LINDDUN engloba 3 etapas principais: (i) modelar o sistema, (ii) identificar ameaças e (iii) gerenciar ameaças. Na primeira etapa, o LINDDUN usa, semelhante ao STRIDE, um diagrama de fluxo de dados (DFD) para capturar o entendimento do funcionamento do sistema e realizar posteriormente uma análise da privacidade. Após o sistema ser descrito, cada elemento do DFD é analisado sistematicamente quanto as potenciais ameaças de privacidade.

A segunda etapa da metodologia utiliza uma tabela personalizada, semelhante a Tabela 2.1, para mapear as ameaças correspondentes aos elementos do DFD criado na etapa anterior. Cada 'X' indicado na tabela do mapeamento é examinado para determinar se representa uma ameaça ao sistema. Para essa análise, o LINDDUN fornece um conjunto de árvores de ameaças de privacidade. Essas árvores representam os caminhos de ataques mais comuns para uma categoria de ameaça LINDDUN associada a um tipo de elemento do DFD. Um exemplo da árvore de ameaça LINDDUN é apresentado na Figura 2.2. Por fim, o LINDDUN fornece uma lista extensa de tecnologias que podem ser utilizadas para gerenciar e mitigar as ameaças elicitadas.

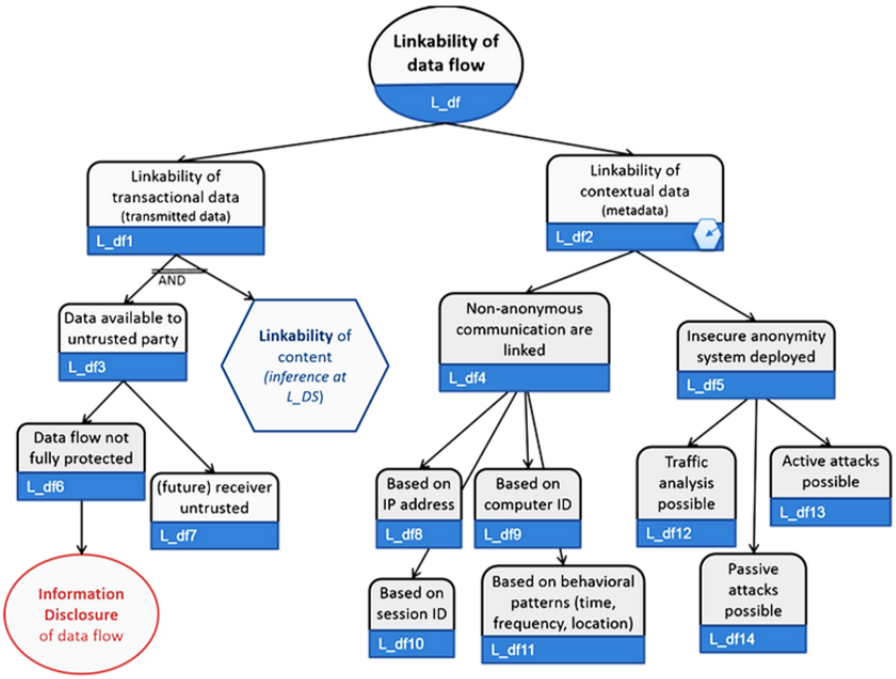


Figura 2.2: Árvore de ameaças LINDDUN - vinculação do fluxo de dados
Fonte: Wuyts et al. (2018)

Embora as metodologias STRIDE e LINDDUN sejam um guia interessante para modelagem de ameaças, estas não se adéquam totalmente ao contexto de RSOs. Ambas foram propostas para mitigar o risco de ameaças associado ao funcionamento e arquitetura de sistemas gerais, ou seja, foram projetadas para tratar das ameaças inseridas neste universo. Isto implica dizer que a preocupação com a proteção de dados do usuário não está no foco central das metodologias. Por exemplo, o modelo de categorização utilizado na fase de identificação de ameaças LINDDUN pode não incluir categorias de ameaças relevantes que possam violar a privacidade do usuário e que estão presentes no contexto atual de RSOs.

Em uma outra perspectiva, UcedaVelez and Morana (2015) propuseram um método para simulação de ataques e análise de ameaças, denominado PASTA (*Process for Attack Simulation and Threat Analysis*). O objetivo central do método é fornecer um processo dinâmico de identificação, enumeração e pontuação de ameaças a um determinado sistema. A metodologia PASTA envolve 7 etapas para apoiar o processo de modelagem de ameaças, a saber: (i) definir os objetivos; (ii) definir o escopo; (iii) decompor a aplicação; (iv) analisar as ameaças ao sistema; (v) analisar as vulnerabilidades e fraquezas do sistema; (vi) modelar os ataques; e (vii) analisar o impacto de riscos. Uma das principais etapas da metologia é a análise detalhada das ameaças identificadas. Essa análise permite determinar os controles e mecanismos apropriados para serem implementados no sistema, bem como possíveis contramedidas.

No geral, PASTA é uma metodologia indicada para organizações que desejam alinhar suas estratégias de negócios com a segurança do produto. Para isso, ela considera as ameaças como sendo um problema de negócios. Em outras palavras, o método foca em fatores como a arquitetura do software, o contexto do negócio e o perfil de uso do sistema e não destina a sua preocupação com a proteção de dados do usuário. Além isso, assim como as metodologias STRIDE e LINDDUN, a metodologia PASTA enfrenta questões similares no que concerne a sua adaptação ao contexto de RSOs pelas mesmas razões citadas previamente.

Diferente das metodologias de modelagem de ameaças citadas anteriormente, Mead et al. (2018) desenvolveram o hTMM (*Hybrid Threat Modeling Method*), um método para a modelagem de ameaças híbridas. A proposta consiste em uma associação de atividades de outros métodos, como o SQUARE (*Security Quality Requirements Engineering Method*), o *Security Cards* e o *Persona non Grata* (PnG) (Denning et al., 2013). Em linhas gerais, o hTMM usa a engenharia de requisitos proposta pelo SQUARE para elicitar, categorizar e priorizar requisitos de segurança. Em seguida, utiliza a técnica PnG para descobrir maneiras pelas quais um sistema pode ser violado para atender aos objetivos de um atacante. Por fim, aplica a técnica de *Security Cards* (cartões de segurança), para eliminar as PnGs consideradas improváveis de acontecer, resumindo os resultados e avaliando formalmente o risco de uma ameaça ocorrer.

Embora apresente um processo de modelagem de ameaças que envolve várias atividades de engenharia de software e design de sistemas, o hTMM não aborda aspectos de privacidade em RSOs. Além disso, assim como outros métodos já citados, o foco principal da modelagem de ameaças hTMM está na segurança dos componentes do sistema, desconsiderando uma potencial atenção com a proteção da privacidade do usuário.

2.4.2 Abordagens para Modelagem de Ameaças no Contexto de RSOs

No cenário de RSOs, poucos trabalhos se voltam à realização de modelagem de ameaças. O trabalho de Sanz et al. (2010) descreve uma metodologia para a modelagem de ameaças, introduzindo elementos relevantes com foco na proteção de aspectos de segurança de RSOs. Inicialmente, os autores realizaram uma adequação de algumas etapas do ciclo de risco de Laorden et al. (2010) como forma de adaptá-las ao contexto de RSOs. Desse modo, a metodologia proposta pelos autores sugere algumas etapas fundamentais para integrar a um contexto de modelagem, como uma análise sobre os ativos do sistema, uma análise sobre as ameaças e ataques ao sistema e recomendações de contramedidas que as RSOs devem implementar para prevenir ataques direcionados ao sistema.

Nessa mesma direção, Wang and Nepali (2015) propuseram um framework para a modelagem de ameaças em RSOs, a partir de uma perspectiva conceitual. A proposta dos autores apresenta algumas etapas relevantes para o contexto da modelagem. Na primeira etapa, deve-se caracterizar 4 componentes do framework, que são compreendidos como elementos fundamentais para uma modelagem de ameaças, como: (i) sites de RSOs; (ii) provedores de RSOs; (iii) usuários de RSOs; e (iv) usuários maliciosos. Dada a

caracterização desses componentes, recomenda-se identificar os diferentes objetivos que usuários maliciosos pretendem realizar. Após isso, deve-se identificar e analisar as vulnerabilidades do sistema, a partir de seis aspectos de segurança, como hardware, sistemas operacionais, políticas de privacidade de RSOs, configurações de privacidade do usuário, relações do usuário e dados do usuário. Em seguida, deve-se realizar uma análise sobre possíveis ameaças e ataques ao sistema e o risco associado. O risco deve ser analisado e priorizado por meio de dois aspectos: probabilidade e impacto.

Os trabalhos propostos por Sanz et al. (2010) e por Wang and Nepali (2015), apresentam abordagens conceituais para a modelagem de ameaças no contexto de RSOs e ressaltam a importância da utilização dessa metodologia como uma solução para problemáticas de segurança e privacidade nesses sistemas. No entanto, as abordagens apresentadas nesses trabalhos apreciam uma perspectiva de cunho conceitual, que pode servir como insumo e base para a proposição de uma metodologia mais completa e aplicável ao contexto de RSOs. Além disso, as propostas não fornecem orientação metodológica para auxiliar designers e outros profissionais de TI que queiram incorporar a modelagem de ameaças de privacidade em RSOs, no nível de design.

2.4.3 Técnicas Auxiliares ao Processo de Modelagem de Ameaças

Árvores de ataques são uma das técnicas mais antigas e difundidas para auxiliar o processo de modelagem de ameaças em diversos tipos de sistemas. Desenvolvida por Bruce Schneider em 1999 (Schneier, 1999), a técnica foi inicialmente proposta com o seu procedimento de aplicação e desde então tem sido combinada com outros métodos e *frameworks*. Árvores de ataque são essencialmente diagramas que descrevem ataques em um sistema em formato de árvores. A raiz da árvore é o objetivo do ataque e as folhas são formas de atingir esse objetivo. Cada meta é representada em uma árvore separada. Normalmente, são necessárias algumas iterações para decompor o objetivo para construir a árvore. Uma vez que todos os nós folha são identificados, marcadores de possibilidade podem ser atribuídos. Para incorporar essas diferentes opções na árvore, os nós AND e OR devem ser usados; os nós AND indicam que ambos os nós devem ser executados para passar para a próxima etapa. Já os nós OR representam todos os outros nós, ou seja, outras possibilidades. Um exemplo de uma árvore de ataques/ameaças pode ser visto na Figura 2.2, apresentado anteriormente na Seção 2.4.1.

O trabalho proposto por Du et al. (2018) utiliza o conceito de árvores de ataque para criar um modelo de árvore de ataque e defesa. O modelo tem como objetivo principal representar, avaliar e prevenir ameaças de segurança e privacidade em RSOs de larga escala. A solução adota uma estrutura hierárquica que descreve um processo de ataque e as contramedidas correspondentes, conforme mostrado na Figura 2.3. O nó raiz da árvore é o objetivo do ataque. Os nós folhas (ataque atômico) são as etapas para concluir o objetivo do ataque, ou seja, revelar a privacidade dos usuários.

Com a árvore estabelecida, para cada evento de ataque atômico é atribuído um valor correspondente, representando sua taxa de sucesso, e o valor raiz representa o nível de risco ao sistema. Para ilustrar ainda mais o processo de ataque, os autores adaptaram o conceito de cadeia de Markov para caracterizar o esforço de um atacante para atingir

seu objetivo malicioso. Os autores também criaram um jogo de ataque-defesa para modelar a interação entre o atacante e o defensor.

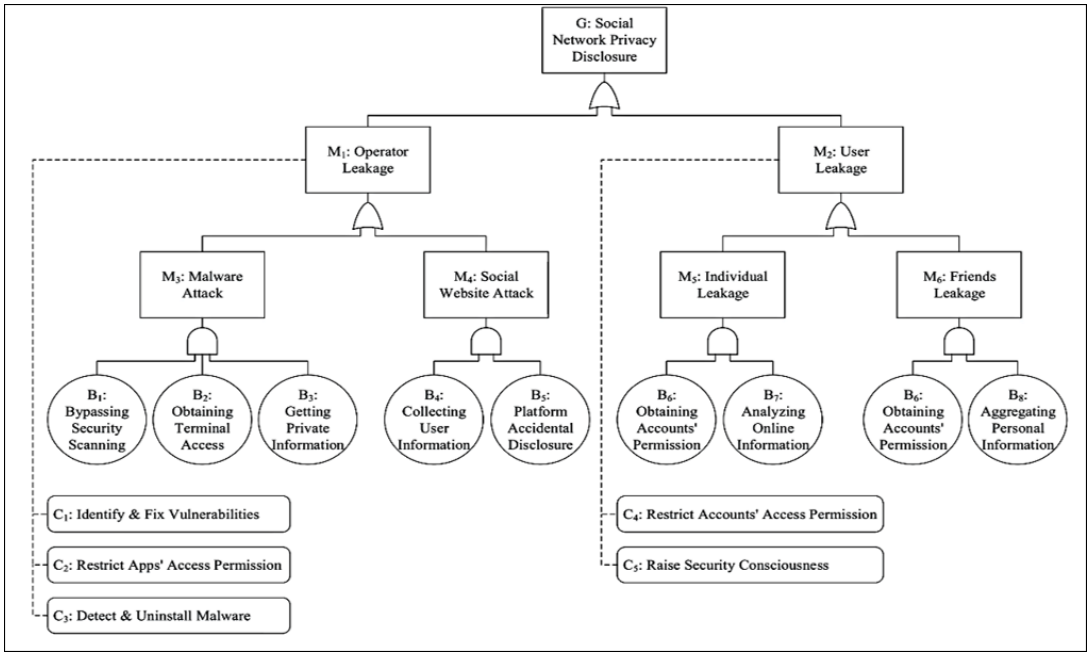


Figura 2.3: Árvore de ataque e defesa para RSOs
Fonte: Du et al. (2018)

As árvores de ataque são fáceis de entender e adotar e são úteis para modelar ameaças relacionadas ao contexto de segurança. Além disso, o método pressupõe que os analistas tenham alto conhecimento em segurança cibernética e, portanto, não fornecem diretrizes para apoiar profissionais que tenham pouco conhecimento em modelagem de ameaças.

A modelagem de ameaças também pode ser aplicada por meio do uso de uma técnica formal para auxiliar o seu processo, que é caso de uso indevido (*misuse cases*) (Alexander, 2003; Sindre and Opdahl, 2005). Os diagramas de casos de uso indevido são semelhantes aos diagramas de casos de uso comum, porém o seu foco central está nas ações do atacante. Os casos de uso indevido têm uma descrição textual, semelhante a especificação de casos de uso, e também podem ser representados por meio de um diagrama, que resume uma sequência de ações de um atacante para um sistema, bem como seu impacto e danos quanto ao uso do sistema. A técnica pode ser utilizada para descobrir e documentar ameaças de segurança ou privacidade. No entanto, trata-se de uma abordagem que não fornece orientação metodológica para descobrir ameaças adicionais e cruciais para o domínio de RSO. A Figura 2.4 ilustra um exemplo do diagrama de caso de uso indevido.

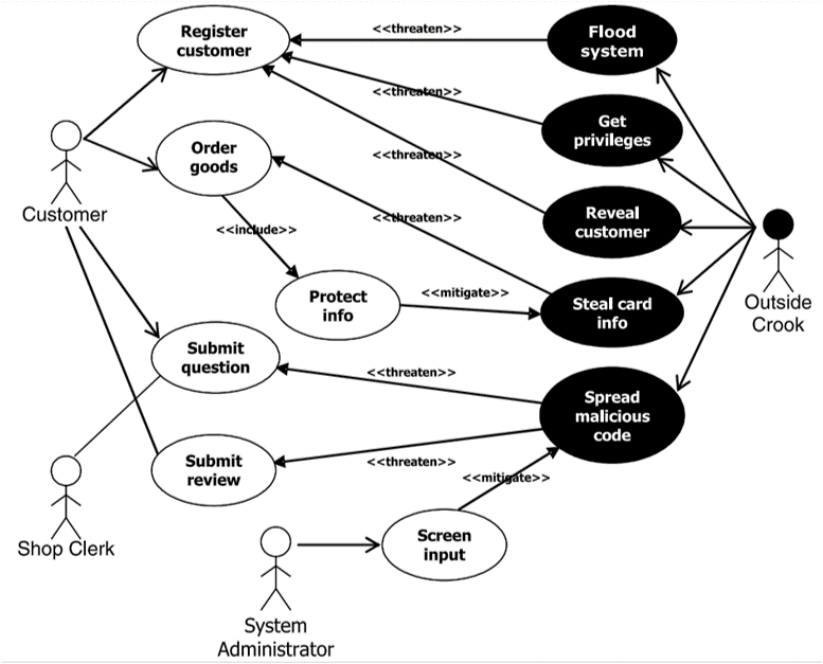


Figura 2.4: Diagrama de caso de uso indevido
Fonte: Sindre and Opdahl (2005)

A Tabela 2.2 compara as metodologias apresentadas, durante a seção de trabalhos relacionados, em termos de foco de interesse, tipo de sistema e contexto para o qual as propostas se destinam. Trabalhos como (Wang and Nepali, 2015; Du et al., 2018) evidenciam a relevância do tratamento de ameaças de segurança para RSOs por meio do mapeamento de taxonomia de ameaças, frameworks, árvores de defesa e ataque, dentre outras contribuições. No entanto, tais trabalhos focam no risco de ameaças e ataques mais relacionados a segurança do funcionamento e arquitetura dos sistemas, não tendo um foco central no principal alvo da violação de privacidade - o usuário. Tais limitações dificultam a reutilização das metodologias e abordagens desses trabalhos para a realização de modelagem de ameaças em RSOs com foco na privacidade do usuário. Desta forma, torna-se clara a necessidade da proposição de novas técnicas e/ou metodologias que visam tratar essas lacunas.

2.5 Considerações sobre o Capítulo

Este capítulo teve como principal objetivo apresentar o aporte teórico acerca do tema abordado neste trabalho, onde foram apresentados os conceitos fundamentais sobre privacidade no contexto de RSOs, ameaças e violações de privacidade e uma definição geral sobre o processo tradicional de modelagem de ameaças. Além disso, foram apresentados conceitos sobre propriedades de privacidade já consolidadas na

Tabela 2.2: Características das principais metodologias para modelagem de ameaças

Metodologias	**Foco**	**Sistema**	**Contexto**
STRIDE (Khan et al., 2017)	Ataque/Prevenção	Genérico	Segurança
LINDDUN (Wuyts et al., 2018)	Ameaça	Genérico	Privacidade
PASTA (UcedaVelez and Morana, 2015)	Risco	Genérico	Segurança
hTMM (Mead et al., 2018)	Ataque/Prevenção	Genérico	Segurança
Modelo de ameaças (Sanz et al., 2010)	Ataque/Prevenção	RSO	Segurança
Framework (Wang and Nepali, 2015)	Ataque/Prevenção	RSO	Segurança
Árvore de ataque (Schneier, 1999)	Ataque	Genérico	Segurança
Árvore de ataque/defesa (Du et al., 2018)	Ataque/Prevenção	RSO	Segurança
Caso de uso indevido (Alexander, 2003)	Ataque	Genérico	Segurança

literatura. Tais propriedades serviram como base para serem inseridas no processo de modelagem proposto nesta pesquisa. Por fim, foram apresentadas as principais metodologias vigentes para a modelagem de ameaças, tanto para contextos genéricos como para RSOs, possibilitando a compreensão do estado da arte do tema de fundo e para identificação das principais lacunas não cobertas por elas.

No geral, os trabalhos relacionados mostraram que metodologias para a modelagem de ameaças estão surgindo, mas não atendem totalmente as expectativas de privacidade em RSOs. Em outras palavras, algumas falham por não fornecer orientação metodológica suficiente para um processo de design de ameaças, outras falham por destinar o foco principal somente na segurança dos componentes do sistema, desconsiderando uma potencial atenção com a proteção dos dados do usuário de RSOs. Para preencher essa lacuna, desenvolvemos a linguagem PTMOL, apresentada no Capítulo 4.

O referencial teórico descrito neste capítulo pode ser considerado um ponto inicial para a construção da PTMOL. No entanto, para tratar ameaças de privacidade em RSOs, tornou-se necessário identificá-las e caracterizá-las de forma mais abrangente. Para isso, realizou-se um mapeamento sistemático da literatura, o qual será descrito no próximo capítulo.

Capítulo 3

Um Mapeamento Sistemático sobre Privacidade em Redes Sociais Online: Ameaças e Soluções

Este capítulo apresenta a condução e os resultados de um mapeamento sistemático da literatura, cujo objetivo consistiu em identificar e caracterizar as ameaças de privacidade mais críticas em RSOs e as soluções vigentes para mitigá-las.

3.1 Introdução

Para propor soluções que apoiem o design de ameaças de privacidade em RSOs, torna-se necessário caracterizar as soluções já existentes na literatura, com o propósito de conhecer as suas propostas e funcionamento, bem como identificar as suas limitações. Com isso, torna-se possível desenvolver um trabalho que esteja devidamente embasado teoricamente e possa agregar conhecimento a área. Por esta razão, decidiu-se realizar um Mapeamento Sistemático da Literatura (MSL).

Um MSL é um tipo de revisão sistemática que visa identificar e classificar os estudos científicos existentes na literatura relacionados a um tópico de interesse de uma área de pesquisa (Kitchenham et al., 2011). Comparado às revisões tradicionais da literatura, o MSL exige maior rigor na sua execução, seguindo um protocolo pré-definido. Assim, seus resultados tendem a ser mais confiáveis, reduzindo a influência do viés dos pesquisadores (Kitchenham et al., 2010; Petersen et al., 2008).

Para a condução do MSL, considerou-se as diretrizes fornecidas por Kitchenham and Charters (2007), as quais foram estruturadas em três etapas: planejamento, execução e relato dos resultados. Na etapa de planejamento, criou-se um protocolo de revisão contendo os seguintes itens: (i) objetivo do MSL; (ii) as questões de pesquisa que o MSL

pretendia responder; (iii) a estratégia utilizada para buscar as contribuições científicas, a qual incluiu as *strings* de busca e os mecanismos de busca, e (iv) os critérios de seleção adotados para determinar quais estudos seriam incluídos ou excluídos no MSL. Esse processo de seleção foi realizado seguindo rigorosamente o protocolo definido. Após a seleção, os dados relevantes identificados nos artigos foram extraídos e os resultados obtidos relatados.

Este capítulo descreve o MSL realizado nesta pesquisa, apresentando seus resultados e discutindo as ameaças de privacidade encontradas, suas definições e soluções para tratá-las. Por fim, com base nos resultados do MSL, um conjunto de ameaças de privacidade em RSOs foi selecionado para ser utilizado como apoio para a proposta da solução formulada nesta pesquisa.

3.2 Protocolo do Mapeamento Sistemático

O protocolo de um MSL especifica os instrumentos que serão utilizados para conduzir o processo específico em torno da execução do MSL e este diminui a possibilidade de viés do pesquisador (Kitchenham and Charters, 2007). Os elementos que compuseram o protocolo do MSL serão descritos em detalhes a seguir.

3.2.1 Objetivo

O objetivo deste MSL está estruturado de acordo com o paradigma GQM *(Goal-Question-Metric)* proposto por Basili and Rombach (1988) e está definido na Tabela 3.1.

Tabela 3.1: Objetivo do MSL segundo paradigma GQM

Analisar as	publicações científicas
com o propósito de	identificar ameaças de privacidade e soluções
com relação a	definição e utilização
do ponto de vista dos	pesquisadores
no contexto de	redes sociais online

3.2.2 Questões de Pesquisa

De acordo com Kitchenham and Charters (2007), a especificação das questões de pesquisa (QPs) é a parte principal de qualquer MSL. De acordo com o objetivo apresentado, as questões de pesquisa definidas neste MSL são apresentadas a seguir:

- QP-1. Quais ameaças de privacidade têm sido consideradas relevantes e precisam ser tratadas no contexto de RSOs?
- QP-2. Quais soluções têm sido adotadas para lidar com as ameaças de privacidade em RSOs?

- QP-3. Que procedimentos metodológicos foram adotados para avaliar as soluções propostas?

A QP-1 visa identificar as ameaças de privacidade existentes no domínio de RSOs, mostrando como elas podem afetar a privacidade dos usuário. A QP-2 visa identificar as soluções vigentes para tratar tais ameaças, bem como suas lacunas. Por fim, a QP-3 busca investigar qual procedimento metodológico foi adotado para avaliar as soluções identificadas. As respostas a essas questões de pesquisa abrangem o estado da arte atual sobre o tema explorado neste trabalho.

3.2.3 Estratégia de busca dos artigos

Em qualquer MSL, o pesquisador deve adotar estratégias e critérios de seleção para incluir publicações relevantes e excluir aquelas que não são relevantes, de acordo com os objetivos e as questões de pesquisa definidos. A estratégia de busca adotada neste MSL considera dois itens: (i) a seleção dos mecanismos de busca; e (ii) o tipo de publicação. Em relação aos mecanismos de busca, as bibliotecas digitais *Elsevier Scopus*[1] e *ACM*[2] foram inicialmente escolhidas para a busca das publicações. Essa escolha deu-se pelo fato de que tais bases de dados indexam publicações de qualidade e relevantes na área de Ciência da Computação. Conduzimos um teste na biblioteca IEEE, porém 75% das publicações eram duplicadas em relação aos resultados da *Scopus* e *ACM*. Além disso, por meio da leitura do título e *abstract* das publicações retornadas, identificamos que os demais 25% não apresentavam soluções que atendiam as questões de pesquisa. Desse modo, a *Engineering Village*[3] foi escolhida como outra alternativa de máquina de busca, pois permite também o uso de expressões lógicas para as buscas automáticas, além de conter uma variedade de publicações relacionadas a engenharia e design de sistemas.

Em relação ao tipo de documento, somente publicações científicas, como artigos de conferências e periódicos, completos ou resumidos, foram consideradas neste MSL. Isso porque esse tipo de documento possui conteúdo revisado por outros pesquisadores independentes, os quais utilizam o método de revisão por pares (*peer review*).

A estratégia de busca também incluiu a definição da *string* de busca a ser utilizada nas bases de dados selecionadas. Para estruturar os termos da *string*, foram utilizados os parâmetros PICOC *(Population, Intervention, Comparison, Output e Context*), sugeridos por Petticrew and Roberts (2008). No entanto, os parâmetros de comparação (*comparison*) e contexto (*context*) não foram utilizados no MSL, uma vez que o objetivo é caracterizar ameaças de privacidade e soluções existentes, portanto não há comparação para determinar o contexto. Os termos utilizados que formam a *string* de busca são apresentados na Tabela 3.2.

[1] https://www.scopus.com
[2] https://www.acm.org
[3] https://www.engineeringvillage.com/

Tabela 3.2: *Strings* de busca utilizadas no MSL

Critério PICOC	*Strings* de busca
População	"online social network" **OR** "social network" **OR** "social software" **OR** "social application" **OR** "social system" **OR** "social interaction") **AND**
Intervenção	"language" **OR** "tool" **OR** "framework" **OR** "technique" **OR** "method" **OR** "mechanism" **OR** "model" **OR** "guideline" **OR** "approach" **OR** "algorithm" **OR** "aspect" **OR** "heuristic") **AND**
Resultado	"privacy threat modelling" **OR** "privacy threat evaluation" **OR** "privacy modeling" **OR** "privacy threat" **OR** "threat modeling" **OR** "privacy risk" **OR** "privacy vulnerability"

3.2.4 Critérios para seleção dos artigos

Os critérios de seleção servem para definir se um artigo será incluído ou excluído do MSL, visando garantir a relevância desses artigos para o contexto da pesquisa. A Tabela 3.3 apresenta os critérios de seleção definidos neste MSL.

Tabela 3.3: Critérios de seleção do artigos

Critérios	Critérios de inclusão
CI-1	O artigo descreve técnicas de modelagem de ameaças de privacidade em RSOs
CI-2	O artigo descreve uma linguagem ou notação para modelagem de ameaças de privacidade em RSOs
CI-3	O artigo descreve soluções para tratar ameaças de privacidade em RSOs
CI-4	O artigo descreve ameaças específicas de privacidade em RSOs
CI-5	O artigo deve descreve estudos experimentais que avaliem uma solução para tratar ameaças de privacidade em RSOs
Critérios	**Critérios de exclusão**
CE-1	O artigo não atende nenhum dos critérios de inclusão
CE-2	A versão completa do artigo não está disponível para download ou nas fontes de busca
CE-3	A publicação não é um artigo científico, por exemplo, é um capítulo de um livro, portanto, não garantindo que houve revisão por pares (*peer review*)
CE-4	O artigo não está em inglês
CE-5	O artigo está duplicado, ou seja, foi retornado em outro mecanismo de busca

3.3 Execução do Mapeamento Sistemático

Para a execução da busca dos artigos, o pesquisador responsável pelo MSL aplicou as *strings* de busca nas bases de dados selecionadas e armazenou o conjunto de referências recuperadas na ferramenta Start[4] para análise posterior. Para garantir

[4]Start: ferramenta de apoio ao planejamento e execução de revisões sistemáticas. Disponível em: http://lapes.dc.ufscar.br/tools/start_tool

a confiabilidade dos resultados obtidos, cada artigo retornado foi analisado por outros dois pesquisadores. Para estruturar o processo de execução do MSL, foi definido um procedimento com três etapas:

- **Processo de seleção preliminar (1º filtro):** Nesta etapa, o pesquisador avaliou o título, resumo e palavras-chave do conjunto de artigos retornado nos mecanismos de busca, de acordo com os critérios de inclusão e exclusão estabelecidos. Em caso de dúvidas sobre alguma publicação, os pesquisadores a mantinham para ser analisada na próxima etapa do processo de seleção.
- **Eliminação por leitura diagonal (2º filtro):** Esta etapa consistiu em uma leitura diagonal (introdução, principais tópicos e conclusão), dos artigos selecionados, para analisar se o mesmo estava associado às questões de pesquisa. Nesta etapa também foram aplicados os critérios de inclusão e exclusão estabelecidos. Em caso de dúvida quanto à exclusão de um determinado artigo, ele permanecia na lista de seleção para ser analisado na etapa seguinte.
- **Processo de seleção final (3º filtro):** Após finalizar o segundo filtro, o terceiro e último filtro foi aplicado. Como a estratégia de ler apenas informações principais (introdução, tópicos principais e conclusão) não é suficiente para identificar se um artigo é realmente relevante para a pesquisa, realizou-se uma leitura completa dos artigos selecionados no segundo filtro. Quaisquer dúvidas sobre as publicações foram discutidas e resolvidas. Esta revisão concluiu o processo de seleção dos artigos.

3.3.1 Procedimento para extração dos dados

O procedimento para a extração de dados empregado neste mapeamento foi baseado em fornecer o conjunto de possíveis respostas para cada questão de pesquisa definida anteriormente. Esse procedimento assegura a aplicação dos mesmos critérios de extração de dados para todos os artigos selecionados e facilita a sua classificação. Os dados extraídos foram registrados em um documento, conforme apresentado na Tabela 3.4, para posterior análise e síntese.

Tabela 3.4: Formulário de extração utilizado no MSL

Itens extraídos	Descrição
Título, autores, ano e objetivo do artigo	Resumo do artigo
QP-1	Descrição da QP-1
QP-2	Descrição da QP-2
QP-3	Descrição da QP-3

3.3.2 Artigos selecionados no MSL

Inicialmente, o MSL foi executado em 2020. Posteriormente, em julho de 2021, uma nova busca foi realizada para abranger novas publicações. Conforme ilustrado

na Figura 3.1, foram retornadas 904 publicações como resultado da busca inicial nas bibliotecas selecionadas (primeiro filtro). Desse total, 428 artigos foram obtidos na biblioteca digital *Scopus*, 373 na *ACM* e os outros 103 na *Engineering Village*. Após a remoção das duplicatas, o número de publicações selecionadas para leitura do título, resumo e palavras-chave (primeiro filtro) foi de 772. Após a aplicação dos critérios de inclusão e exclusão nessas publicações, 149 artigos foram selecionados para a aplicação do segundo filtro. Todas as 149 publicações foram lidas por meio da leitura diagonal (introdução, tópicos principais, conclusão), e apenas 55 publicações atenderam aos critérios de inclusão. Por fim, após a leitura completa desses artigos (terceiro filtro), um total de 43 artigos foram selecionados para a extração de dados.

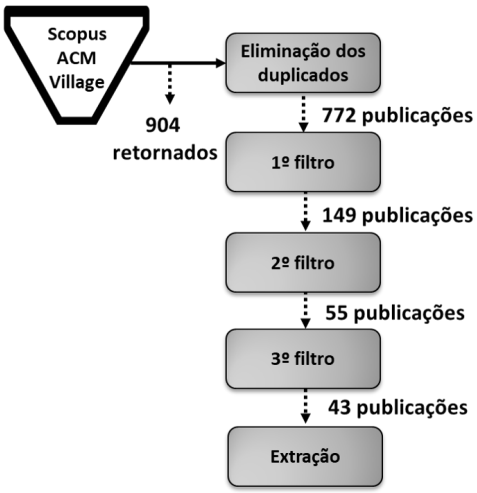


Figura 3.1: Resultado do processo de seleção dos artigos
Fonte: Próprio Autor.

A Tabela 3.5 lista o conjunto de artigos selecionados neste mapeamento. Os artigos estão identificados com os códigos (A1, A2...), que representam a ordem de numeração dos mesmos. No final do título de cada artigo é apresentada a máquina de busca a qual o mesmo foi identificado.

Tabela 3.5: Artigos selecionados no Mapeamento Sistemático

Código	Referências	Título dos artigos
A1	(Alrayes et al., 2020)	Modelling perceived risks to personal privacy from location disclosure on online social networks [SCOPUS]
A2	(Alemany et al., 2019b)	Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms [SCOPUS]

continua na próxima página

Tabela 3.5 – continuação da página anterior

Código	Referências	Título dos artigos
A3	(Al-Asmari and Saleh, 2019a)	A Conceptual Framework for Measuring Personal Privacy Risks in Facebook Online Social Network [SCOPUS]
A4	(Alemany et al., 2019a)	Metrics for Privacy Assessment When Sharing Information in Online Social Networks [SCOPUS]
A5	(Wen et al., 2018)	A Privacy Analysis Method to Anonymous Graph Based on Bayes Rule in Social Networks [SCOPUS]
A6	(Ferreyra et al., 2017)	At your own risk: shaping privacy heuristics for online self-disclosure [SCOPUS]
A7	(Song et al., 2018)	A personal privacy preserving framework: I let you know who can see what [SCOPUS]
A8	(De and Imine, 2018a)	To reveal or not to reveal: balancing user-centric social benefit and privacy in online social networks [SCOPUS]
A9	(Du et al., 2018)	Modeling privacy leakage risks in large-scale social networks [SCOPUS]
A10	(Abid et al., 2018b)	Online testing of user profile resilience against inference attacks in social networks [SCOPUS]
A11	(De and Imine, 2018b)	Privacy Scoring of Social Network User Profiles through Risk Analysis [SCOPUS]
A12	(Abawajy et al., 2018)	Privacy threat analysis of mobile social network data publishing [SCOPUS]
A13	(Rathore et al., 2017)	Social network security: Issues, challenges, threats, and solutions [SCOPUS]
A14	(Pensa and Di Blasi, 2017)	A privacy self-assessment framework for online social networks [SCOPUS]
A15	(Aktypi et al., 2017)	Unwinding Ariadne's identity thread: Privacy risks with fitness trackers and online social networks [SCOPUS]
A16	(Puglisi et al., 2017)	On the anonymity risk of time-varying user profiles [SCOPUS]
A17	(Jin et al., 2012)	Towards understanding location privacy awareness on geo-social networks [SCOPUS]
A18	(Kumar et al., 2017)	Risk analysis of online social networks [SCOPUS]
A19	(Abawajy et al., 2016a)	Privacy preserving social network data publication [SCOPUS]
A20	(Dong and Zhou, 2016)	Privacy Inference Analysis on Event-Based Social Networks [SCOPUS]
A21	(Tucker et al., 2015)	Privacy pal: improving permission safety awareness of third party applications in online social networks [SCOPUS]
A22	(Zeng et al., 2015)	A study of online social network privacy via the tape framework [SCOPUS]
A23	(Wang and Nepali, 2015)	Privacy threat modeling framework for online social networks [SCOPUS]

continua na próxima página

Tabela 3.5 – continuação da página anterior

Código	Referências	Título dos artigos
A24	(Jaafor et al., 2015)	Privacy threats from social networking service aggregators [SCOPUS]
A25	(Li et al., 2015)	Privacy leakage analysis in online social networks [SCOPUS]
A26	(Fogues et al., 2015)	Open challenges in relationship-based privacy mechanisms for social network services [SCOPUS]
A27	(Li, 2015)	A privacy preservation model for health-related social networking sites [SCOPUS]
A28	(Casas et al., 2015)	Social network privacy: Issues and measurement [SCOPUS]
A29	(Zhang et al., 2014)	Privacy risk in anonymized heterogeneous information networks [SCOPUS]
A30	(Mahmood, 2012)	New privacy threats for facebook and twitter users [SCOPUS]
A31	(Erlandsson et al., 2012)	Privacy threats related to user profiling in online social networks [SCOPUS]
A32	(Sramka, 2012)	Privacy scores: assessing privacy risks beyond social networks [SCOPUS]
A33	(Akcora et al., 2012)	Privacy in social networks: How risky is your social graph? [SCOPUS]
A34	(Watanabe et al., 2011)	PrIvacy risks and countermeasures in publishing and mining social network data [SCOPUS]
A35	(Ninggal and Abawajy, 2011)	Privacy threat analysis of social network data [SCOPUS]
A36	(Kavianpour et al., 2011)	Effectiveness of using integrated algorithm in preserving privacy of social network sites users [SCOPUS]
A37	(Tang et al., 2011)	Need for symmetry: Addressing privacy risks in online social networks [SCOPUS]
A38	(Laorden et al., 2010)	A threat model approach to threats and vulnerabilities in online social networks [SCOPUS]
A39	(Cheung and She, 2016)	Evaluating the privacy risk of user-shared images [ACM]
A40	(Korolova et al.)	Link privacy in social networks [ACM]
A41	(Williams, 2010)	Social networking applications in health care: threats to the privacy and security of health information [ACM]
A42	(Biega et al., 2016)	R-susceptibility: An ir-centric approach to assessing privacy risks for users in online communities [ACM]
A43	(Jaafor and Birregah, 2015)	Multi-layered graph-based model for social engineering vulnerability assessment [Village]

3.4 Resultados

Esta seção apresenta os resultados obtidos após a execução do MSL. Para responder as questões de pesquisa definidas previamente, a subseção 3.4.1 apresenta o conjunto de ameaças identificado no MSL, demonstrando suas consequências para a privacidade do usuário de RSOs. A subseção 3.4.2 apresenta as soluções existentes para mitigação de ameaças de privacidade. Por fim, a subseção 3.4.3 mostra quais procedimentos metodológicos foram adotados para avaliar as soluções identificadas.

3.4.1 QP-1. Quais ameaças de privacidade têm sido consideradas relevantes e precisam ser tratadas no contexto de RSOs?

À medida que os usuários confiam cada vez mais nas RSOs para suas atividades de comunicação, diversas informações pessoais são disponibilizadas publicamente. Essas informações podem ser usadas para atividades maliciosas como fraudes sociais, roubo de identidade ou disseminação de dados (Rathore et al., 2017; Dong and Zhou, 2016; Joyee De and Imine, 2019). Conforme visto no capítulo 2, uma ameaça de privacidade é um evento indesejável potencial ou real que pode causar divulgação, exposição e uso indevido de dados privados (Joyee De and Imine, 2019; Laorden et al., 2010). No entanto, não está claro quais são as ameaças de privacidade mais críticas no domínio de RSOs. Essa limitação é exatamente o que esta questão de pesquisa pretende responder.

Para identificar e extrair as ameaças mais críticas de privacidade existentes na literatura, realizou-se uma análise minuciosa nos artigos encontrados no MSL. Essa análise teve como objetivo realizar um levantamento inicial sobre as principais ameaças descritas pelos autores dos artigos, observando sua relevância e impacto para a privacidade do usuário. É importante ressaltar que nem todos os artigos identificados no MSL apontavam ameaças potenciais, alguns apresentavam uma solução para mitigá-las. Como a QP-1 buscou investigar as ameaças em si, e não as soluções existentes para tratá-las, buscou-se realizar uma análise somente nos artigos do MSL que descreviam ameaças de privacidade com detalhes específicos. Isso permitiu uma melhor compreensão para chegar em uma lista precisa de ameaças. Cada artigo foi analisado e as ameaças abordadas neles foram extraídas.

Após esse levantamento inicial, criou-se um diagnóstico com mais de 30 ameaças de privacidade. Ao observar o diagnóstico inicial, notou-se que diversas ameaças incluídas nele eram de natureza igual ou semelhante, ou seja, estavam descritas com nomenclaturas diferentes, mas continham o mesmo significado. Outras ameaças eram relacionadas a segurança de sistemas e seu foco não estava relacionado efetivamente com a privacidade dos dados do usuário. Para compreender melhor o conjunto de ameaças e chegar a um diagnóstico mais preciso, as principais ameaças (aquelas mais citadas no MSL e consideradas mais críticas para a privacidade do usuário) foram separadas em uma categoria principal e reunidas com seus sinônimos, ou seja, aquelas ameaças com nomes diferentes, mas com o mesmo significado. Esta análise pode ser vista na Tabela 3.6.

Com base no diagnóstico de ameaças extraído a partir do mapeamento, criou-se um catálogo final registrando as ameaças de privacidade mais críticas no contexto de

Tabela 3.6: Lista das principais ameaças de privacidade identificadas no MSL

Ameaças	Sinônimos	Referências
Cyberstalking	Stalking Digital stalking	(De and Imine, 2018a) (Aktypi et al., 2017) (Fogues et al., 2015) (Sramka, 2012)
Divulgação de informação	Disseminação Divulgação de conteúdo Divulgação de identidade Uso indevido de dados	(Rathore et al., 2017) (Aktypi et al., 2017) (Zeng et al., 2015) (Bioglio et al., 2019) (Casas et al., 2015)
Clonagem de perfil	Perfil falso Perfil clonado	(Rathore et al., 2017) (Abid et al., 2018b) (Aktypi et al., 2017) (Mahmood, 2012) (Jaafor and Birregah, 2015)
Inferência ou Rastreamento	Extração de informações Rastreamento de atividades Mineração de dados Criação de perfil	(Laorden et al., 2010) (Watanabe et al., 2011) (Wang and Nepali, 2015) (Abid et al., 2018b) (Dong and Zhou, 2016)
Ameaça à reputação	Discriminação Constrangimento Ataques Sybil Manipulação de dados	(Rathore et al., 2017) (Aktypi et al., 2017)
Reconhecimento facial	Recuperação de imagens Marcação de fotos	(Laorden et al., 2010) (Kumar et al., 2017) (Kavianpour et al., 2011)
Espionagem	Espionagem corporativa Monitoramento	(Aktypi et al., 2017)
Gravação não autorizada	Risco de videochamadas Videochamadas em grupo	(Rathore et al., 2017)
Roubo de identidade	Phishing Invasão de conta Descoberta de atributos ocultos	(De and Imine, 2018a) (Al-Asmari and Saleh, 2019a) (De and Imine, 2018b) (Tucker et al., 2015) (De and Imine, 2018a) (Al-Asmari and Saleh, 2019a) (De and Imine, 2018b) (Tucker et al., 2015)

RSOs, citadas na literatura. Essas ameaças podem impactar fortemente a privacidade do usuário na forma de divulgação, manipulação ou uso indevido de dados privados. Ressalta-se que antes de chegar no catálogo final de ameaças, várias revisões e refinamentos foram realizados pelo autor da pesquisa e seus coautores, de modo a consolidar o artefato final. Cada ameaça do catálogo é descrita a seguir:

- **Cyberstalking** - Uso da RSO para assediar ou perseguir um indivíduo, ou um grupo de indivíduos, com comportamento indesejado ou ameaçador, imposto repetidamente (De and Imine, 2018a; Aktypi et al., 2017; Fogues et al., 2015;

Sramka, 2012). Os usuários revelam de forma frequente dados pessoais em seus perfis. Um agente malicioso pode coletar esses dados para usá-los indevidamente para cyberstalking.

- **Divulgação de Informação** - Refere-se à descoberta e divulgação não autorizada de informações privadas. Essa divulgação pode expor diretamente uma enorme quantidade de dados pessoais do usuário, entre endereço residencial, dados relacionados à saúde, dados de rotina, de relacionamento, dentre outros. O compartilhamento dessas informações pode causar implicações negativas para a privacidade do usuário, como o uso indevido desses dados para fins diversos, como campanha política, marketing e anúncios indesejados (Rathore et al., 2017; Aktypi et al., 2017; Zeng et al., 2015; Bioglio et al., 2019; Casas et al., 2015).

- **Clonagem de perfil** - Um agente malicioso pode utilizar os dados compartilhados por um determinado usuário e clonar o seu perfil, sem que a RSO ou a própria vítima percebam a clonagem. Com isso, o agente malicioso cria uma identidade falsa para fazer os amigos da vítima acreditarem no novo perfil (falso). Com esse perfil criado, o agente malicioso poderá entrar em contato com a lista de amigos da vítima e enviar links para capturar dados privados (Rathore et al., 2017; Abid et al., 2018b; Aktypi et al., 2017; Mahmood, 2012; Jaafor and Birregah, 2015).

- **Inferência ou rastreamento** - É a coleta e combinação de dados para gerar ou descobrir informações pessoais do usuário que não estão diretamente compartilhadas em seus perfis nas RSOs, mas podem ser inferidas usando diferentes técnicas computacionais. Além disso, os provedores da RSO rastreiam e analisam as atividades online do usuário (como navegação diária e preferências de compras, por exemplo) por meio de diversas técnicas de aprendizagem de máquina. Como resultado, as RSOs constroem perfis completos do usuário com o objetivo de vender produtos ou rastrear o seu comportamento. Tudo isso feito sem o conhecimento do usuário. (Laorden et al., 2010; Watanabe et al., 2011; Wang and Nepali, 2015; Abid et al., 2018b; Dong and Zhou, 2016).

- **Ameaça à reputação** - Devido às RSOs permitirem que indivíduos compartilhem diversas informações pessoais, seus usuários podem ser vítimas de danos à reputação. Um agente malicioso ou uma entidade maliciosa pode obter acesso a informações íntimas e explorá-las para prejudicar a privacidade do usuário (Rathore et al., 2017; Aktypi et al., 2017). Além disso, os usuários podem se tornar vítimas de manipulação e distorção de dados. Atualmente, existem diversas ferramentas disponíveis para manipular e distorcer diversos dados.

- **Reconhecimento facial** - A maioria das RSOs permitem o compartilhamento de fotos. Os algoritmos de reconhecimento facial são capazes de identificar ou verificar uma pessoa a partir de uma imagem ou de uma fonte de vídeo. Identificar o rosto de uma pessoa em uma foto ou vídeo e fazer referência cruzada com outros dados pode ser usado para expor informações pessoais do usuário. Algoritmos

combinados com outras tecnologias permitem encontrar usuários com uma boa precisão, sem o seu consentimento (Laorden et al., 2010; Kumar et al., 2017; Kavianpour et al., 2011). Recentemente, o jornal americano *New York Times* publicou uma matéria sobre a empresa Clearview AI, que opera um aplicativo de reconhecimento facial. A Clearview criou um banco de dados com mais de três bilhões de imagens de usuários das RSOs Facebook e YouTube e usou esse banco de dados para identificar pessoas em outras imagens.

- **Espionagem** - É um tipo de monitoramento que permite, em tempo real, a coleta e o processamento de diversas atividades do usuário de RSOs, espionando principalmente suas atividades de perfil e relacionamentos com outros indivíduos (Aktypi et al., 2017). Essa espionagem é uma ameaça social em que as atividades são frequentemente monitoradas nesses sistemas (Ali et al., 2019). Uma das principais preocupações surge quando essa ameaça é explorada pelo governo, podendo realizar o monitoramento de cidadãos ou de adversários, visando atacá-los (Aktypi et al., 2017).

- **Gravação não autorizada** - Atualmente, muitas RSOs fornecem serviços de *chat* e videochamadas, proporcionando mais interação entre seus usuários. No entanto, muitas informações pessoais podem ser divulgadas ou coletadas via videochamada. Um dos participantes pode facilmente realizar uma gravação não autorizada para posteriormente chantagear o outro participante (vítima). Além disso, um participante pode distorcer os dados da chamada e exibi-los inadequadamente (Rathore et al., 2017).

- **Roubo de identidade** - É um tipo de ameaça em que um agente malicioso obtém acesso ilegal a conta do usuário da RSO para capturar dados privados (De and Imine, 2018a; Al-Asmari and Saleh, 2019a; De and Imine, 2018b; Tucker et al., 2015; De and Imine, 2018a; Al-Asmari and Saleh, 2019a; De and Imine, 2018b; Tucker et al., 2015). Diferentes técnicas maliciosas podem ser aplicadas por um atacante para realizar um roubo de identidade. Por exemplo, um atacante pode enviar links para obter informações confidenciais, como senhas e códigos de autenticação. De posse desses dados, poderá obter acesso a conta do usuário na RSO e todo seu registro de atividades e dados pessoais.

A resposta para a QP-1 é concluída apresentando as principais ameaças de privacidade citadas na literatura, que podem ser utilizadas por fontes de vazamento para divulgar ou usar de forma indevida os dados privados do usuário. Dados privados são alvos desejáveis para agentes maliciosos, pois, de posse deles, eles podem descobrir informações confidenciais, como senhas, códigos de autenticação e até dados financeiros. Da mesma forma, o conteúdo compartilhado pelo usuário pode ser combinado com outros conjuntos de dados públicos usando técnicas de mineração de dados. Com isso, um perfil completo do usuário pode ser construído, o que pode comprometer ainda mais a sua privacidade.

Além disso, algumas das ameaças apresentadas acima mostram que um agente malicioso pode explorar diversos recursos da RSO e interagir com diferentes tipos de usuários, como menores de idade e funcionários corporativos. Muitos danos podem ocorrer quando essas ameaças são executadas, como chantagem, compartilhamento de pornografia, assédio e espionagem. A defesa contra essas ameaças é fornecida por meio de configurações de privacidade e controles de acesso. No entanto, a eficácia desses mecanismos nem sempre é suficiente, pois muitos são projetados na forma de um acordo com os usuários para coletar mais informações sobre eles, em vez de proteger de forma efetiva a sua privacidade. Na próxima seção, são apresentadas e discutidas as principais soluções acadêmicas identificadas no MSL, que podem ser usadas para mitigar ameaças de privacidade.

3.4.2 QP-2. Quais soluções têm sido adotadas para lidar com as ameaças de privacidade em RSOs?

Nos últimos anos, o interesse e o esforço em desenvolver soluções preventivas para tratar ameaças de segurança e privacidade em RSOs aumentou (Rathore et al., 2017; Yassein et al., 2019; Deliri and Albanese, 2015; Ali et al., 2019). Nesta subseção, será apresentada uma visão geral das diferentes soluções identificadas no MSL e suas estratégias para mitigar os efeitos de ameaças em RSOs. No geral, algumas soluções focam em uma perspectiva conceitual, explicando as características ou comportamento das ameaças de privacidade em RSOs por meio de um modelo. Outras soluções foram desenvolvidas visando aumentar a conscientização do usuário sobre as consequências relacionadas à divulgação de suas informações, permitindo que eles tomem decisões mais preventivas quanto a sua privacidade. Por fim, outras soluções foram projetadas para quantificar, medir e avaliar ameaças e riscos de privacidade em RSOs. A Tabela 3.7 apresenta um resumo dessas soluções, seus tipos e estratégias adotadas.

Tabela 3.7: Resumo das soluções existentes para lidar com ameaças de privacidade

Referências	Nome da solução	Tipo de solução	Estratégia adotada
Du et al. (2018)	Attack Defensive Tree	Modelo	Árvores de ataque e cadeia de Markov
Song et al. (2018)	TOKEN	Modelo	Aprendizagem de Máquina
Aktypi et al. (2017)	Identity-Exposure	Ferramenta	Inferências
Abid et al. (2018b)	SONSAI	Ferramenta	*Random walks and Word2Vec algorithm*
Tucker et al. (2015)	Privacy Pal	Ferramenta	Estimativa de risco
Ferreyra et al. (2018)	PHeDer	Método	Heurísticas de privacidade

continua na próxima página

Tabela 3.7 – continuação da página anterior

Referências	Nome da solução	Tipo de solução	Estratégia adotada
De and Imine (2018b)	Privacy Scoring	Mecanismo	Análise de risco e árvores de danos
Tang et al. (2011)	Reverse Lookup	Algoritmo	Redes bayesianas
Kavianpour et al. (2011)	Integrated Algorithm	Algoritmo	Algoritmos de k-anonimato e k-diversidade
Wen et al. (2018)	Bayesian Analysis Model	Algoritmo	Redes bayesianas
Alrayes et al. (2020)	MPRLS	Ferramenta	Ferramentas de feedback
Al-Asmari and Saleh (2019a)	Abordagem conceitual	Framework	Métricas
Pensa and Di Blasi (2017)	Abordagem Conceitual	Framework	Aprendizagem Ativa
Sramka (2012)	Privacy score	Métricas	Análise de risco e algoritmos de inferência
Alemany et al. (2019a)	Audience and Reachability	Métrica	*Friendship layer model*
Zeng et al. (2015)	TAPE	Framework	Métricas, Algoritmos e Análise de sensibilidade
Puglisi et al. (2017)	Modelo conceitual	Modelo	Risco de anonimato
Alemany et al. (2019b)	Nudging mechanisms	Mecanismo	Estimativa de Risco
Biega et al. (2014)	R-Susceptibility	Modelo	Ranking e modelos de tópicos latentes
Jaafor et al. (2015)	Abordagem	Algoritmo	Árvore de decisão
Akcora et al. (2012)	Risk learning	Algoritmo	Aprendizagem de máquina
Wang and Nepali (2015)	Abordagem conceitual	Framework	Modelagem de Ameaças

Os resultados apresentados nessa subseção respondem a questão de pesquisa (QP-2), indicando diversos trabalhos que propuseram soluções acadêmicas para proteger os usuários contra inúmeras ameaças de privacidade. A maioria das soluções identificadas direcionam o foco da sua proposta principalmente para a prevenção e medição de riscos associados a ameaças de privacidade. No entanto, observou-se que ainda existem

limitações e algumas lacunas não cobertas pelas soluções existentes, que podem ser relevantes para a proposta de novas soluções. As principais lacunas observadas nas soluções vigentes identificadas no MSL, indicam que:

- Muitos pesquisadores desenvolveram soluções para proteger os usuários contra ameaças de privacidade Wang and Nepali (2015); Du et al. (2018); Alrayes et al. (2020); Erlandsson et al. (2012). No entanto, não houve uma identificação clara em como antecipar a preocupação com ameaças de privacidade nos estágios que antecedem o desenvolvimento de sistemas de RSOs. Isso demonstra que a maioria das soluções consideram o tratamento de ameaças em um estágio posterior do desenvolvimento de aplicações sociais, sendo que poucos esforços são dados para tratar ameaças em nível de design. A busca antecipada por ameaças às quais um usuário poderá está exposto pode permitir que uma equipe de projeto determine de forma mais eficaz quais controles de privacidade uma RSO precisa definir para reduzir os efeitos e consequências dessas ameaças. Esse esforço pode tornar as RSOs muito mais protegidas e, ao priorizar as ameaças previstas, os mecanismos e contramedidas de privacidade são implementados de forma mais assertiva.

- Existem várias soluções para medir ou avaliar o risco de ameaças de privacidade em RSOs. Essas soluções incluem modelos de inferência (Abid et al., 2018a), análise de sensibilidade (Zeng et al., 2014) e métricas para quantificar, medir e estimar riscos de privacidade (Al-Asmari and Saleh, 2019b; Alemany et al., 2019a; Zhang et al., 2017). No entanto, várias das métricas utilizadas para cálculos e estimativas foram desenvolvidas para reduzir os riscos de ameaças relacionadas ao funcionamento e arquitetura geral desses sistemas, não apresentando um foco específico para a proteção de dados do usuário.

- Somente o trabalho de Wang and Nepali (2015) apresentou, por meio de uma perspectiva conceitual, elementos e definições para uma modelagem de ameaças com foco no contexto de RSOs. No entanto, a proposta dos autores não fornece orientação metodológica para auxiliar designers e outros profissionais de TI que queiram incorporar a modelagem de ameaças em RSOs, no nível de design. Além disso, por apresentar uma abordagem conceitual, o framework pode servir como base para a proposição de uma metodologia mais completa para modelagem de ameaças de privacidade orientada a RSOs.

3.4.3 QP-3. Que procedimentos metodológicos foram adotados para avaliar as soluções propostas?

Esta questão de pesquisa tem como principal objetivo apresentar quais os principais procedimentos metodológicos que foram adotados para avaliar as soluções identificadas no MSL. A Tabela 3.8 apresenta um resumo das principais características dos estudos relatados nas publicações, destacando a metodologia adotada no contexto do estudo, a métrica de avaliação utilizada e o *dataset* (se houver) usado para testar a solução.

Tabela 3.8: Características dos procedimentos metodológicos adotados para avaliar as soluções

Referência	Solução	Metodologia	Métrica	Dataset
Du et al. (2018)	Modelo	Simulação	Z-test e Matriz de transição	Facebook, Twitter e Myspace
Song et al. (2018)	Framework	Simulação	S@K e P@K	Twitter
Aktypi et al. (2017)	Ferramenta	Estudo empírico	Usabilidade	N/A
Abid et al. (2018b)	Ferramenta	Simulação	Acurácia	Facebook
Tucker et al. (2015)	Ferramenta	Estudo com usuário	Eficácia	N/A
De and Imine (2018a)	Modelo	Simulação	Viabilidade	N/A
Tang et al. (2011)	Algoritmo	Simulação	Variações de probabilidade de inferência	N/A
Kavianpour et al. (2011)	Algoritmo	Simulação	Eficácia	N/A
Wen et al. (2018)	Modelo	Simulação e Viabilidade	Gráfico de rede aleatório	N/A
Alrayes et al. (2020)	Modelo	Survey com usuários	Viabilidade	N/A
Pensa and Di Blasi (2017)	Framework	Simulação	Sesibilidade e Visibilidade	Naive Bayes classifier
Sramka (2012)	Framework	Estudo de caso	Viabilidade	N/A
Alemany et al. (2019a)	Abordagem	Simulação	Acurácia e utilidade	N/A
Zeng et al. (2015)	Abordagem	Simulação	Conscientização e Confiança	Facebook
Puglisi et al. (2017)	Modelo	Simulação	Viabilidade	Facebook
Alemany et al. (2019b)	Abordagem	Survey	Pontuação de risco	N/A
Biega et al. (2014)	Abordagem	Simulação	Precisão	AOL, Health Forums and Quora
Jaafor et al. (2015)	Abordagem	Survey	Pontuação de privacidade	N/A
Akcora et al. (2012)	Abordagem	Simulação	Eficácia	N/A

Das 22 soluções identificadas, 19 avaliaram sua proposta utilizando os procedimentos metodológicos apresentados na Tabela 3.8. Com isso, observou-se que a maioria das soluções foram avaliadas por meio de simulações, não sendo testadas ou utilizadas em projetos reais na indústria ou em outras organizações. Além disso, nota-se que há uma carência na adoção de instrumentos de coleta de dados qualitativos, como entrevistas ou grupos focais. Tais instrumentos poderiam trazer informações que não buscam apenas medir a solução, mas também descrevê-la, usando impressões e opiniões.

3.5 Ameaças à Validade

Todo estudo possui ameaças que podem afetar a validade dos seus resultados (Wohlin et al., 2012). Dentre as ameaças à validade deste estudo, destacam-se duas principais. A primeira ameaça está relacionada com a possibilidade do autor deste estudo ter introduzido seu viés durante a execução do protocolo do MSL, a qual foi mitigada pelo acompanhamento e revisão por outros pesquisadores mais experientes durante o processo de execução. A outra ameaça relacionada a validade de conclusão desse MSL é a generalização dos resultados, mitigada pela escolha de duas meta-bibliotecas digitais, que indexam outras bibliotecas digitais de diferentes áreas do conhecimento, incluindo áreas onde a privacidade é um tópico recorrente.

3.6 Considerações do Capítulo

Este capítulo apresentou um mapeamento sistemático da literatura sobre ameaças de privacidade em RSOs e soluções existentes para mitigá-las. Após a execução de três filtros nos artigos analisados, foram selecionados um total de 43 publicações que atendiam aos critérios de inclusão estabelecidos. Com base no MSL executado, criou-se um catálogo, que indica as ameaças mais críticas no contexto de RSOs, citadas na literatura. Esse catálogo foi gerado a partir de uma análise minuciosa realizada nos artigos identificados no MSL. Os resultados indicam que as ameaças de privacidade existentes são mais utilizadas para cumprir os seguintes objetivos: a) coletar informações pessoais sobre um determinado usuário, como nome, sexo, localização, fotos e vídeos privados, atividades e interesses online; e b) obter dados do perfil do usuário e utilizar esses dados como meio de divulgação para atingir os amigos do usuário e capturar suas informações confidenciais. Em geral, essas ameaças são exploradas para divulgar, expor, modificar ou utilizar de forma indevida dados privados armazenados ou compartilhados em RSOs.

Uma das consequências mais críticas que podem ocorrer por meio da prática de ameaças de privacidade é o roubo de identidade. Nessa ameaça, um atacante rouba os dados confidenciais de um usuário, como seu nome completo, número de telefone e endereço, sem sua permissão, para realizar crimes cibernéticos, como golpes ou fraudes. No entanto, nem sempre ameaças relacionadas ao conteúdo que o usuário publica podem ocorrer. Um atacante pode simplesmente acessar a lista de amigos/seguidores de um determinado usuário e simular ser um amigo em comum, visando obter informações pessoais do usuário. Além disso, as RSOs estão construindo perfis completos sobre diversos usuários com a intenção de vender produtos e registrar o seu comportamento. Esse rastreamento e análise das atividades geralmente são feitos sem o conhecimento do usuário, trazendo implicações relevantes para a sua privacidade.

Os resultados do MSL também revelaram diversos estudos propondo soluções acadêmicas para proteger os usuários contra inúmeras ameaças de privacidade. Tais soluções são classificadas principalmente como soluções de prevenção e medição de riscos associados às ameaças em RSOs. No entanto, essas abordagens, no geral, são direcionadas para mitigar ameaças e vulnerabilidades e reduzir os riscos relacionados

ao funcionamento e arquitetura desses sistemas. Além disso, ainda existem limitações por parte das soluções vigentes no que se refere ao design de ameaças de privacidade em RSOs que permite a antecipação, ainda em nível de design, dos cenários de ameaças aos quais um usuário poderá estar potencialmente exposto.

Uma solução não deve somente atender aos requisitos funcionais e ajudar a resolver os problemas do sistema, deve também focar no usuário, pois ele é o principal alvo de ameaças e violações de privacidade. Desta forma, torna-se necessário propor novas soluções que visem tratar essa lacuna, pois, até o presente momento, não foram identificadas propostas de modelagem de ameaças de privacidade com foco central no usuário, que possibilite a sua utilização mais amplamente no domínio de RSOs. Essa lacuna é mitigada por meio da linguagem PTMOL, que será apresentada no próximo capítulo.

Capítulo 4

PTMOL - Privacy Threat MOdeling Language

Este capítulo apresenta a linguagem proposta para a modelagem de ameaças de privacidade em RSOs, denominada Privacy Threat MOdeling Language (PTMOL). Inicialmente, são apresentadas as atividades que foram necessárias para o desenvolvimento da solução. Posteriormente, é fornecida uma visão geral da linguagem proposta e também são apresentadas as definições de cada atividade envolvida nas etapas do processo de modelagem de ameaças de privacidade aplicável ao contexto de RSOs.

4.1 Introdução

Antecipar a preocupação com ameaças de privacidade para as etapas iniciais do desenvolvimento de RSOs é uma estratégia importante no sentido de incorporar a proteção de dados pessoais do usuário nos estágios iniciais do ciclo de desenvolvimento desses sistemas. Embora existam propostas de modelagem de ameaças para sistemas gerais (UcedaVelez and Morana, 2015; Potteiger et al., 2016; Wuyts et al., 2018), tais abordagens são limitadas para prever ameaças de privacidade no contexto de RSOs em nível de design. Algumas dessas limitações são descritas a seguir.

As contribuições identificadas nos trabalhos relacionados presentes na literatura e no mapeamento sistemático executado nessa pesquisa (Capítulo 3) apresentam diversas soluções para modelar ou mitigar o risco de ameaças e ataques mais relacionados a segurança do funcionamento e arquitetura de sistemas gerais, não tendo um foco central no principal alvo da violação de privacidade, o usuário. Tais limitações dificultam a reutilização dessas soluções para a realização de uma modelagem efetiva de ameaças em RSOs com foco na privacidade do usuário. Dessa forma, torna-se clara a necessidade da proposição de novas soluções que visam tratar essas lacunas.

Como possível solução para tais problemas identificados, foi desenvolvida uma linguagem para a modelagem de ameaças em RSOs, com foco específico na privacidade do usuário. Essa linguagem visa reduzir as limitações das soluções existentes, uma

vez que nenhum dos trabalhos relacionados identificados na literatura consideram os dados do usuário como o foco central do processo de modelagem. Na próxima seção, são apresentadas as atividades que foram efetuadas no processo de desenvolvimento da solução.

4.2 Processo de desenvolvimento da PTMOL

A Figura 4.1 apresenta as principais atividades utilizadas para o desenvolvimento da solução proposta neste trabalho. As atividades envolvidas no processo foram: (i) revisão do estado da arte; (ii) identificação e análise das limitações dos trabalhos existentes; (iii) inserção, adaptação e exclusão de elementos; e (iv) refinamento da solução. Cada atividade é descrita a seguir.

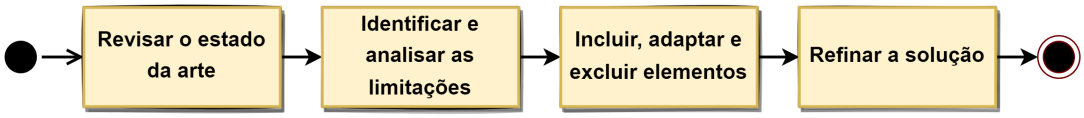


Figura 4.1: Processo de desenvolvimento da linguagem PTMOL
Fonte: Próprio autor.

4.2.1 Revisão do estado da arte

Para conhecer em mais profundidade as soluções que tratavam sobre ameaças de privacidade no contexto de RSOs, tornou-se necessário identificá-las e caracterizá-las, de modo que fosse possível obter um entendimento sobre o estado da arte no que se refere às principais metodologias de modelagem de ameaças existentes. A partir da observação da literatura, buscou-se a identificação dessas metodologias e uma visão das atividades envolvidas no processo de modelagem proposto por elas. Nessa atividade, foram consideradas tanto as metodologias para contextos generalistas quanto as metodologias ou trabalhos que utilizam modelagem de ameaças no contexto de RSOs. Esses trabalhos, assim como suas respectivas descrições e detalhes, podem ser consultados no Capítulo 2.

4.2.2 Identificação das limitações

Como estratégia para a proposição de uma nova solução aplicável ao contexto de RSOs, buscou-se caracterizar as abordagens já existentes na literatura, com o propósito de conhecer seus funcionamentos bem como identificar as suas limitações. As atividades das metodologias vigentes foram mapeadas e analisadas. Com isso, foi possível diagnosticar as principais limitações das soluções e os *gaps* não cobertos por elas.

No geral, observou-se que muitas das soluções existentes foram desenvolvidas para reduzir os riscos de ameaças relacionados a segurança do funcionamento e arquitetura de sistemas gerais e continham características que dificultavam sua aplicação,

ou não eram suficientes, para uma modelagem de ameaças com foco na privacidade do usuário. Essa questão indica uma limitação considerável, pois uma solução não deve somente atender aos requisitos funcionais e ajudar a resolver os problemas do sistema, deve também focar no usuário, uma vez que ele é o principal alvo da violação de privacidade. A partir dessa estratégia, alguns elementos base da modelagem de ameaças foram extraídos e posteriormente analisados.

4.2.3 Inclusão, adaptação e exclusão de elementos

Para construir a estrutura inicial da solução, os elementos que integravam a metodologia de modelagem de ameaças foram previamente analisados em termos de adequação ao contexto de privacidade em RSOs. Esses elementos foram alvos de três decisões estratégicas: exclusão do elemento, adaptação do elemento e inserção de um novo elemento. Elementos excluídos foram aqueles considerados não aplicáveis ao domínio de RSOs e que não envolviam aspectos de privacidade. Os elementos adaptados foram aqueles que necessitaram de modificações para serem incluídos na modelagem de ameaças de privacidade orientada a RSOs. Por fim, os elementos inseridos foram aqueles que não pertenciam à modelagem de ameaças tradicional e foram incluídos na nova solução. Para garantir a confiabilidade da análise realizada, cada elemento foi analisado por outros dois pesquisadores. A Tabela 4.1 apresenta o resultado das decisões adotadas em relação aos elementos supracitados. A partir disso, uma nova linguagem para modelagem de ameaças de privacidade em RSOs foi elaborada. A linguagem foi denominada PTMOL (*Privacy Threat MOdeling Language*).

Tabela 4.1: Resultado das decisões adotadas em relação aos elementos da modelagem de ameaças

Elementos	Estratégia adotada	Justificativa
Ativo	Adaptado	Conceito adaptado para o foco nos ativos do usuário
Ameaça	Adaptado	Conceito adaptado para o foco em ameaças para a privacidade do usuário
Vulnerabilidade	Excluído	Aborda conceitos relacionados à falhas de segurança
Exploit	Excluído	Aborda conceitos relacionados a aspectos de segurança
Risco	Excluído	O objetivo da solução não é avaliar ou medir riscos
Contramedida	Adaptado	Conceito associado com propriedades de privacidade
Ataque	Excluído	Trata sobre problemas de segurança
Usos maliciosos	Inserido	Elemento inserido com o foco em prever usos maliciosos para os ativos do usuário

continua na próxima página

Tabela 4.1 – continuação da página anterior

Elemento	Estratégia adotada	Justificativa
Fontes de vazamento	Inserido	Caracteriza os principais agentes da ameaça
Alerta de prevenção	Inserido	Elemento inserido como uma estratégia de conscientização ao usuário
Zona de compartilhamento	Inserido	Elemento de representação de um espaço do sistema
Zona de risco	Inserido	Elemento de representação de um espaço do sistema
Zona de vazamento	Inserido	Elemento de representação de um espaço dentro ou fora do sistema

4.2.4 Refinamento da solução

Após a criação da linguagem para modelagem de ameaças com foco na privacidade do usuário, tornou-se necessário testá-la para obter *insights* sobre sua viabilidade prática. Para tal, foram realizados estudos empíricos que possibilitaram que a proposta fosse refinada para a sua melhor adequação ao contexto de RSOs. Esses estudos são apresentados no Capítulo 5.

4.3 PTMOL - Uma linguagem de apoio a modelagem de ameaças de privacidade em RSOs

Para apoiar projetistas a antecipar os cenários de ameaças aos quais um usuário poderá está potencialmente exposto, foi desenvolvida uma linguagem para a modelagem de ameaças de privacidade em RSOs, denominada *Privacy Threat Modeling Language* (PTMOL). A PTMOL pode ser incorporada ao desenvolvimento de RSOs durante a fase de design. É importante ressaltar que o processo de modelagem proposto pela linguagem não busca identificar falhas ou problemas de interação e interface no projeto de privacidade de RSOs, o objetivo é fazer um levantamento detalhado de todas as ameaças que podem comprometer a privacidade do usuário. Tal procedimento tende a ser cada vez mais demandado pelas RSOs, principalmente por conta da adequação com leis gerais de proteção de dados.

Para fins de introdução geral, é importante conhecer e compreender o propósito da PTMOL, sua estrutura e aplicação. A PTMOL é uma linguagem de apoio a modelagem de ameaças de privacidade em nível de design. Trata-se de uma linguagem porque pode ser utilizada para expressar o conhecimento em uma estrutura que é definida por um conjunto consistente de regras. Com isso, permite que designers de RSOs identifiquem possíveis ameaças de privacidade, suas consequências e como elas podem ser mitigadas. Para realizar esse suporte, a PTMOL possui recursos para o design de ameaças e permite gerar um modelo de ameaças como parte do design. Por ser uma linguagem, a PTMOL é formada pelos seguintes componentes: (a) um vocabulário; (b)

a sintaxe; e (c) a semântica. O vocabulário é a coleção de todas as palavras à disposição do designer que podem ser usadas no processo de modelagem. A sintaxe é o conjunto consistente de regras da linguagem, indicando como elas podem ser empregadas durante o processo de modelagem. Por fim, a semântica refere-se ao significado associado aos elementos da linguagem. Quanto ao seu vocabulário, a PTMOL possui os seguintes termos:

- **Ativo**. Atributo relacionado ao alvo (usuário) que possui um valor pessoal.
- **Ameaça**. Uma situação indesejada que pode colocar em risco os ativos do usuário.
- **Fontes de vazamento**. Fontes que operam dentro ou fora do sistema para violar a privacidade do usuário. Podem ser classificadas como:
  - Um **membro malicioso** infiltrado na própria RSO do usuário, que pode ser um amigo ou um seguidor;
  - O próprio **provedor de serviços**, que pode fazer uso indevido dos dados privados armazenados na rede;
  - Um **aplicativo terceirizado**, que tem acesso ou faz uso indevido dos dados do usuário;
  - **Fontes externas**, que não estão diretamente infiltradas nas RSOs, mas conseguem coletar e obter dados do usuário vinculados em outros sites, como mecanismos de busca, por exemplo.
- **Usos maliciosos**. Descreve os usos maliciosos previstos que podem afetar a privacidade do usuário.
- **Alerta de prevenção**. Alerta do sistema para informar os usuários sobre qualquer ação que pode causar violações graves para a sua privacidade.
- **Contramedida**. Ações do sistema para mitigar ameaças de privacidade executadas pelas fontes de vazamento.
- **Zona de compartilhamento**. Representa um espaço do sistema onde os ativos do usuário podem ser compartilhados ou coletados.
- **Zona de risco**. Representa um espaço do sistema no qual pode ocorrer ameaças de privacidade.
- **Zona de vazamento**. Representa a porta de acesso indevido aos dados privados do usuário.

Com base no vocabulário da PTMOL, criou-se um conjunto de elementos e regras que determinam a sintaxe da linguagem. Esses elementos e seus relacionamentos são ilustrados na Figura 4.2, agrupados segundo a sua zona: zona de compartilhamento, zona de risco e zona de vazamento. Tais elementos podem ser utilizados ao final do processo para gerar o modelo de ameaças resultante da modelagem.

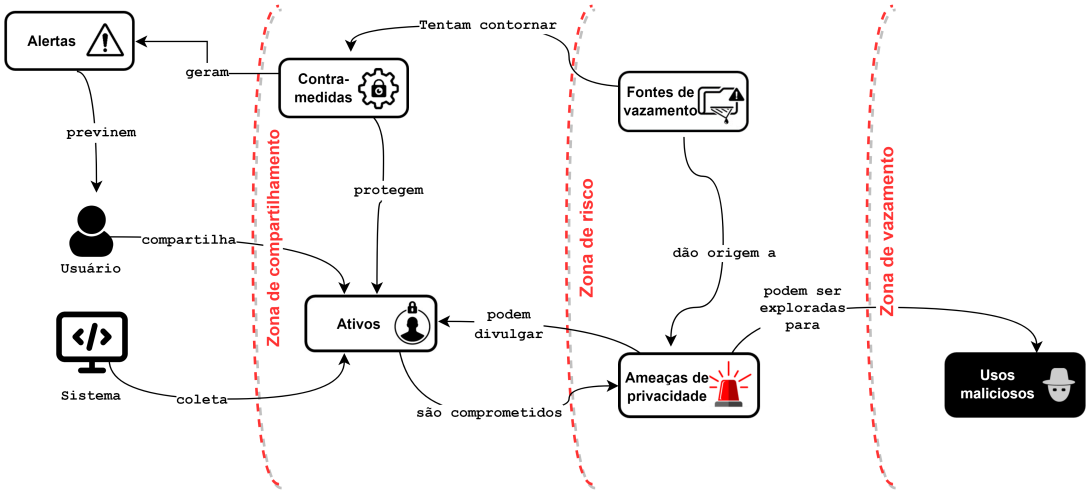


Figura 4.2: Visão geral sobre as relações entre os elementos da PTMOL
Fonte: Próprio autor.

4.3.1 Atividade do processo de design em que a PTMOL pode ser aplicada

Em linhas gerais, as atividades do processo de design podem ser caracterizadas como (Barbosa and Silva, 2010): (i) análise da situação atual ou do problema, onde o designer deve buscar estudar e interpretar uma boa forma de melhorar uma ou mais características da situação atual do sistema; (ii) síntese de uma intervenção, onde deve-se planejar e executar uma intervenção na situação atual; e (iii) avaliação de nova situação, na qual deve-se comparar a situação analisada anteriormente com a nova situação, atingida após a intervenção.

De acordo com Barbosa and Silva (2010) a diferença entre a situação atual e uma situação desejada é a motivação principal para projetar e sintetizar uma intervenção. Em outras palavras, uma intervenção é denominada de solução, pois responde a pergunta que define um problema a ser resolvido: “Como melhorar esta situação?”. Sob esta ótica, a PTMOL pode ser aplicada no processo de design tanto em uma atividade de análise, para identificar previamente todas as ameaças que podem comprometer a privacidade do usuário, quanto na atividade de síntese de intervenção, de modo a selecionar estratégias de mitigação que possam reduzir os efeitos das ameaças, executando uma intervenção na situação atual.

4.3.2 Recursos de apoio à modelagem

Para apoiar o processo de modelagem de ameaças, a PTMOL dispõe de um conjunto de recursos. O primeiro recurso estabelecido é o catálogo de ameaças, o qual descreve as ameaças mais críticas para a privacidade do usuário (Figura 4.3). Elas foram descobertas a partir de uma investigação profunda feita por meio de um mapeamento sistemático (Capítulo 3). Esse catálogo de ameaças é um recurso de grande

valor, pois ajuda o designer a refletir sobre quais cenários de ameaça um usuário está potencialmente exposto. Além disso, esse recurso também possibilita ao designer prever usos maliciosos que podem colocar em risco os ativos do usuário. A Figura 4.4 apresenta a descrição da ameaça de "inferência ou rastreamento de dados". O catálogo completo pode ser visualizado no Apêndice B.

Figura 4.3: Catálogo de ameaças da PTMOL
Fonte: Próprio autor.

Um segundo recurso previsto para auxiliar o processo de modelagem é a taxonomia de contramedidas (Figura 4.5), que pode ser utilizada para prevenir ou mitigar os efeitos das ameaças. Essas contramedidas foram adaptadas a partir do conjunto de propriedades de ameaças apresentadas no capítulo 2 e servem como um aporte para auxiliar na formulação de estratégias preventivas para mitigar as ameaças identificadas. Os designers têm a possibilidade de construir estratégias de mitigação, que podem ser fornecidas posteriormente à equipe de desenvolvimento, para considerá-las durante a construção da aplicação. As estratégias de mitigação adotadas são:

- **Desvinculação**. Refere-se a capacidade de ocultar o vínculo (relação) entre duas ou mais ações, identidades ou informações do usuário. O agente malicioso não pode ser capaz de identificar se dois itens estão relacionados.
- **Anonimato**. O atacante não pode ser capaz de identificar um indivíduo dentro de um conjunto de indivíduos anônimos.

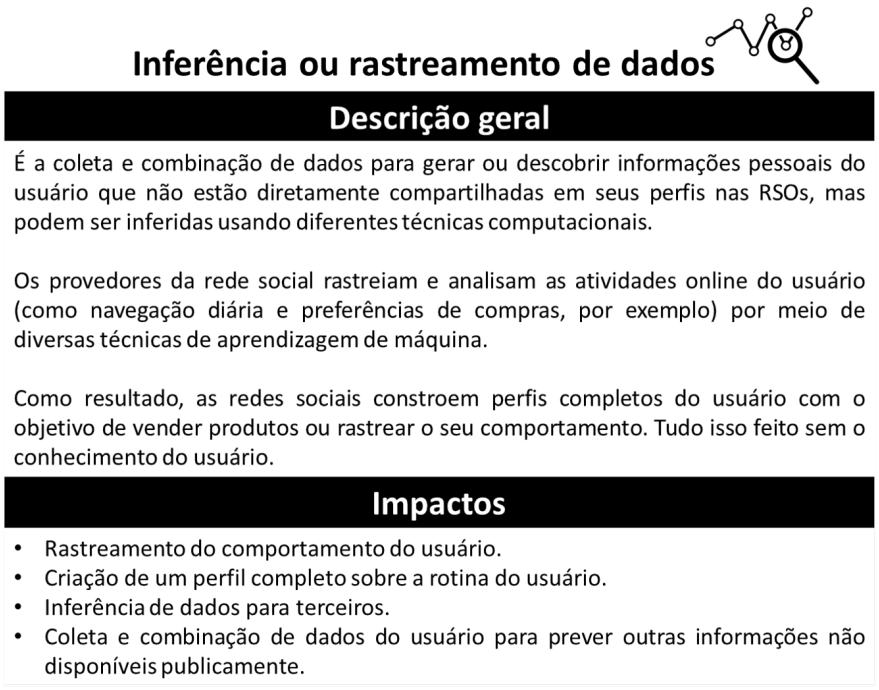


Figura 4.4: Descrição da ameaça “inferência ou rastreamento de dados”
Fonte: Próprio autor.

- **Confidencialidade**. Refere-se a ocultação dos conteúdos dos dados do usuário ou liberação controlada desses conteúdos. No geral, a confidencialidade significa preservar as restrições de acesso e divulgação de informações.
- **Não detecção**. Refere-se a ocultação das atividades do usuário. Por exemplo, um atacante não pode ter a capacidade de distinguir de forma precisa se alguém ou ninguém está em um determinado local.
- **Negação plausível**. Refere-se à capacidade de negar ter realizado uma ação que outras partes não podem confirmar nem contradizer. Em outras palavras, um agente malicioso não pode provar que um usuário sabe, fez ou disse algo. Por exemplo, caso o usuário faça uma denúncia, eles vão querer negar ter enviado uma determinada mensagem para proteger sua privacidade.
- **Conscientização**. Garantir que os usuários têm conhecimento sobre a coleta do seus dados pessoais e que apenas as informações necessárias devem ser utilizadas para permitir o desempenho da funcionalidade dos sistemas.
- **Transparência**. Exige que todo o sistema que armazena dados do usuário informe o titular dos dados sobre a política de privacidade do sistema e permita que o titular dos dados especifique consentimentos em conformidade com a legislação, antes que os usuários acessem o sistema.

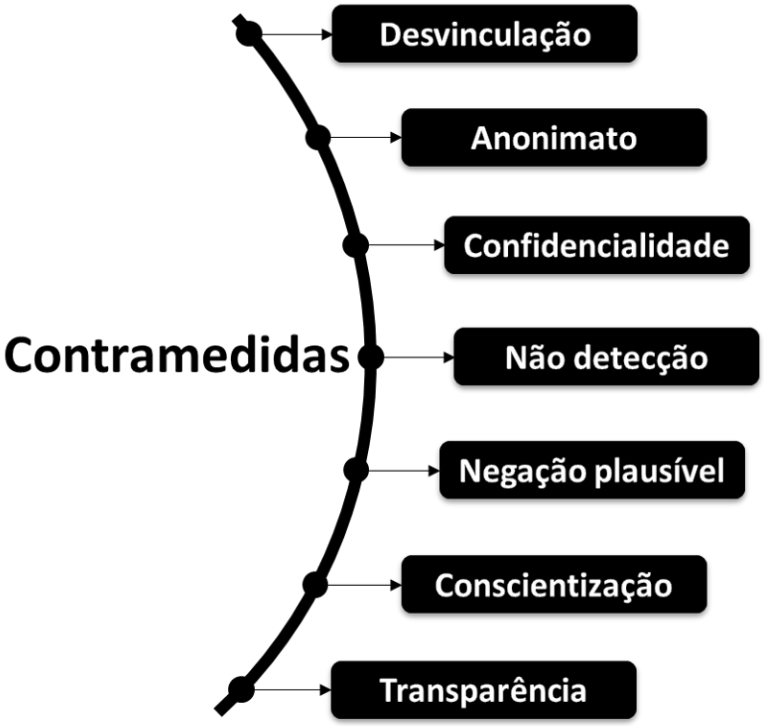


Figura 4.5: Taxonomia de contramedidas da PTMOL
Fonte: Próprio autor.

4.3.3 Processo de aplicação

A Figura 4.6 ilustra o funcionamento do processo de aplicação da PTMOL. A PTMOL permite que o designer represente e, consequentemente, elabore e refine seu projeto em camadas, ou seja, aos poucos. Inicialmente, o designer (Figura 4.6 (a)) deve compreender o domínio da RSO que deseja solucionar. É necessária uma descrição dos recursos que permitem o usuário compartilhar informações no sistema ou de um eventual cenário de interação, onde o usuário compartilhará ativos no sistema.

Após entender um possível cenário de ameaças ao qual o usuário poderá está exposto, a PTMOL possibilita que o designer defina trechos da sua modelagem de ameaças a partir de padrões, ou *templates,* integrados à linguagem, de modo que sua compreensão sobre o problema e possíveis soluções se amplie. O *template* de modelagem (Figura 4.6 (b)) serve como apoio para uma representação estruturada de todas as informações que afetam a privacidade do usuário. Além disso, o *template* permite documentar todas as descobertas, para que futuras alterações no ambiente de interação do sistema possam ser avaliadas rapidamente. O *template* ainda desempenha uma outra função de grande valor: ele auxilia a compreensão sobre a lógica de design subjacente ao processo de modelagem. Após a análise de todas essas informações, o designer deverá produzir o modelo de ameaças (Figura 4.6 (c)) resultante do projeto.

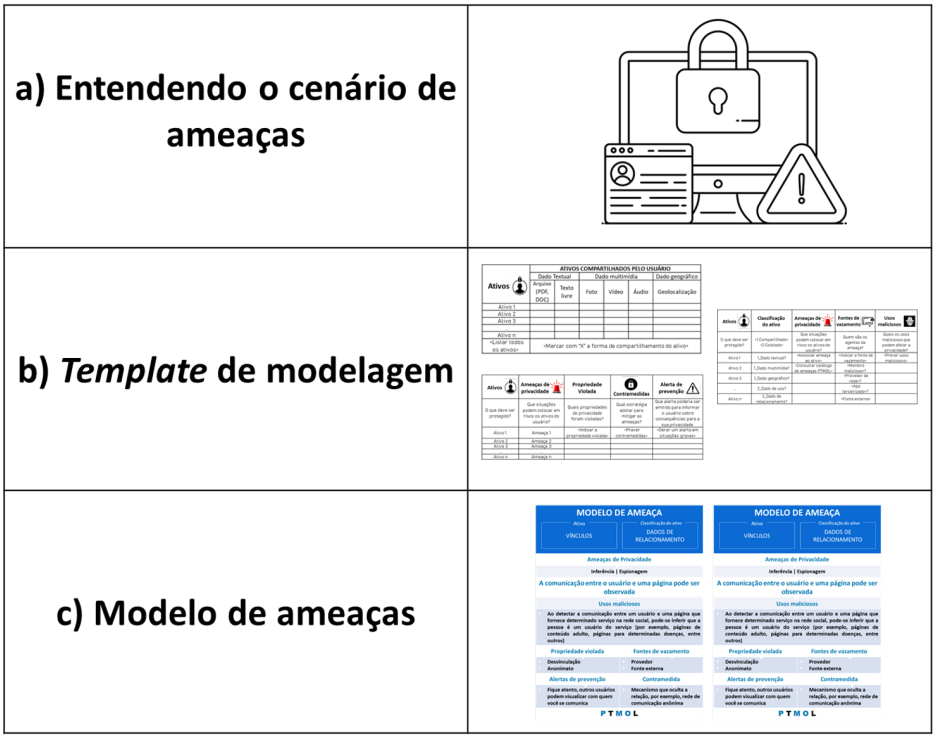


Figura 4.6: Processo de Aplicação da PTMOL
Fonte: Próprio autor

O processo de aplicação da PTMOL permite dividir um processo complexo em tarefas menores, facilitando a identificação de todo o cenário de ameaças. Assim, para iniciar a modelagem de ameaças via *template*, o designer terá que seguir um conjunto atividades para identificar: (i) o que é necessário proteger do usuário (ativos), (ii) quais eventos indesejáveis (ameaças) podem ocorrer e colocar em risco os ativos do usuário; e (iii) quais estratégias adotar (contramedidas) para prevenir ou mitigar os efeitos das ameaças aos dados do usuário. Para algumas etapas da PTMOL existe um conjunto pré-definido de valores para o preenchimento do *template* de modelagem, onde o designer pode indicar um valor do conjunto conforme sugerido pela sintaxe da linguagem. Em outras etapas, o designer pode preencher livremente o *template* de modelagem, podendo indicar valores com base em seu raciocínio ou levando em consideração decisões tomadas pela equipe de design. Essas etapas do processo de modelagem serão descritas em detalhes a seguir. O Apêndice A apresenta um guia prático sobre o processo de modelagem de ameaças da PTMOL.

4.3.3.1 Identificação de ativos

Nesta etapa, o designer deverá identificar os ativos a serem protegidos. Um ativo é algo relacionado ao alvo (usuário) que possui um valor pessoal. Nesta visão, o

designer precisa compreender o que deve ser protegido, antes de começar a descobrir quais ameaças podem ocorrer. É essencial que o designer tenha um entendimento sobre os ativos, pois as próximas etapas da modelagem serão direcionadas a eles. Dependendo da forma como o ativo foi compartilhado no sistema, diferentes ameaças podem ocorrer. Nesta visão, três valores foram definidos:

- Dados textuais: arquivos ou texto livre;
- Dados multimídia: fotos, áudios ou vídeos;
- Dados geográficos: geolocalização.

A Figura 4.7 apresenta o *template* para a classificação de ativos com as suas regras de preenchimento. O *template* permite que o designer liste todos os ativos extraídos do cenário de ameaças e classifique a sua forma de compartilhamento a partir do conjunto pré-definido de valores. Dependendo de como ativo foi compartilhado na RSO, diferentes ameaças podem surgir. Por exemplo, a localização descrita de forma textual é diferente da geolocalização.

Ativos	ATIVOS COMPARTILHADOS PELO USUÁRIO					
	Dado Textual		Dado multimídia			Dado geográfico
	Arquivo (PDF, DOC)	Texto livre	Foto	Vídeo	Áudio	Geolocalização
Ativo 1						
Ativo 2						
Ativo 3						
...						
Ativo n						
<Listar todos os ativos>	<Marcar com "X" a forma de compartilhamento do ativo>					

Figura 4.7: *Template* para a classificação dos ativos compartilhados pelo usuário
Fonte: Próprio autor.

Existem ativos que não são diretamente compartilhados pelos usuários, mas são coletados ou gerados pelo próprio sistema. No geral, os provedores das RSOs rastreiam e analisam as atividades do usuário e constroem perfis completos com propósito de vender produtos e rastrear o seu comportamento. Nesse sentido, duas formas de coleta foram definidas, conforme ilustrado na Figura 4.8. Os ativos coletados pela própria plataforma podem assumir dois valores:

- Dados de uso: atividades, preferências ou comportamento do usuário na RSO;
- Dados de relacionamento: vínculo e relações do usuário com outros.

Ativos	ATIVOS COLETADOS PELO SISTEMA	
	Dados de uso	Dados de relacionamento
Ativo 1		
Ativo 2		
Ativo 3		
...		
Ativo n		
<Listar todos os ativos>	<Marcar com "X" se o ativo pertencer a essa categoria>	<Marcar com "X" se o ativo pertencer a essa categoria>

Figura 4.8: *Template* para a classificação dos ativos coletados pelo sistema
Fonte: Próprio autor.

4.3.3.2 Identificação de ameaças, fontes de vazamento e usos maliciosos

A segunda etapa pode ser considerada como a principal na execução do processo de modelagem de ameaças com a PTMOL. Neste estágio, o designer deve consultar o catálogo de ameaças integrado à linguagem e identificar, a partir de um conjunto pré-definido de valores, quais delas podem ocorrer em relação a cada ativo em análise. Para cada ativo listado, deve-se apontar uma ou mais ameaças de privacidade do catálogo. Após isso, o designer deve indicar as fontes de vazamento que operam dentro ou fora do sistema para violar a privacidade do usuário. Essas fontes podem assumir quatro valores: (i) membro malicioso; (ii) provedor; (iii); app terceirizado; e (iv) fontes externas. Após a associação da ameaça ao ativo e da indicação das fontes de vazamento, o designer deve prever os usos maliciosos, cujo preenchimento tem valor livre. A Figura 4.9 apresenta o *template* para a identificação de ameaças, fontes de vazamento e usos maliciosos previstos.

Ativos	Classificação do ativo	Ameaças de privacidade	Fontes de vazamento	Usos maliciosos
O que deve ser protegido?	Ativo coletado ou compartilhado?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	Valor pré-definido	Valor pré-definido	Valor pré-definido	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Classificar ativo>	<Associar ameaça [do catálogo] ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>

Figura 4.9: *Template* para identificar ameaças, fontes de vazamento e usos maliciosos
Fonte: Próprio autor.

4.3.3.3 Identificação de estratégias de mitigação

Por fim, na última etapa, o designer terá que tomar decisões estratégicas que garantam uma maior assertividade na implantação de alertas e contramedidas adequadas para a proteção dos ativos. Após listar o conjunto de ameaças e suas consequências para a privacidade do usuário, o designer deve consultar a taxonomia implementada com propriedades de privacidade. Com isso, o designer deverá indicar, por meio de uma marcação de seleção "X", quais propriedades foram violadas, conforme mostrado na Figura 4.10.

Ameaça de privacidade 	Qual propriedade de privacidade pode ser violada?						
	Desvinculação	Anonimato	Negação plausível	Não detecção	Confidencialidade	Conscientização	Transparência
Ameaça 1	X					X	
Ameaça 2		X					
Ameaça 3			X				X
...				X		X	
Ameaça n		X			X		

Figura 4.10: *Template* para identificar propriedades de privacidade violadas
Fonte: Próprio autor.

Para cada propriedade indicada como possivelmente violada, torna-se necessário transformá-la posteriormente em contramedida, de modo que esta possa reduzir ou dificultar os usos maliciosos previstos. Além disso, o designer também tem a opção de emitir alertas para informar os usuários sobre qualquer ação que pode causar violações graves para a sua privacidade. Com isso, o designer poderá pensar em contramedidas apropriadas para o sistema, permitindo a antecipação, ainda em fase de design, de decisões estratégicas para a proteção dos dados do usuário. A Figura 4.11 ilustra o *template* de aplicação da etapa 3.

4.3.3.4 Geração do modelo de ameaças

A Figura 4.12 ilustra um modelo de ameaças representando o resultado de uma modelagem aplicada sobre o ativo "vínculos". O modelo gerado serve como um resumo do design de ameaças realizado via *template*. Com base na visão fornecida pelo modelo, nota-se que, para o contexto do ativo coletado, duas ameaças potenciais podem ocorrer: Inferências ou Espionagem. A partir dessas ameaças, o designer pode indicar as fontes de vazamento e os usos maliciosos que podem afetar a privacidade do usuário. Poderá

Ativos	Ameaças de privacidade	Propriedade Violada	Contramedidas	Alerta de prevenção
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quais propriedades de privacidade foram violadas?	Qual estratégia adotar para mitigar as ameaças?	Que alerta poderia ser emitido para informar o usuário sobre consequências para a sua privacidade.
Ativo 1	Valor pré-definido	Valor pré-definido	Valor livre	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Listar todas as ameaças>	<Indicar a propriedade violada>	<Prever contramedidas>	<Gerar um alerta em situações graves>

Figura 4.11: *Template* para identificação de estratégias de mitigação
Fonte: Próprio Autor.

indicar também propriedades de privacidade violadas, potenciais alertas de prevenção e contramedidas que possam dificultar o reduzir os efeitos da ameaça.

4.4 Considerações sobre o capítulo

Este capítulo apresentou a linguagem proposta para a modelagem de ameaças de privacidade em RSOs, denominada *Privacy Threat Modeling Language* (PTMOL). Foram apresentadas as principais atividades envolvidas para o desenvolvimento da solução. Além disso, o capítulo forneceu uma visão geral da PTMOL, definindo cada etapa do processo de modelagem de ameaças proposto pela linguagem. O próximo capítulo apresenta o processo de avaliação e evolução da PTMOL por meio da condução de um conjunto de estudos empíricos, que teve o propósito realizar os procedimentos de validade e confiabilidade da mesma.

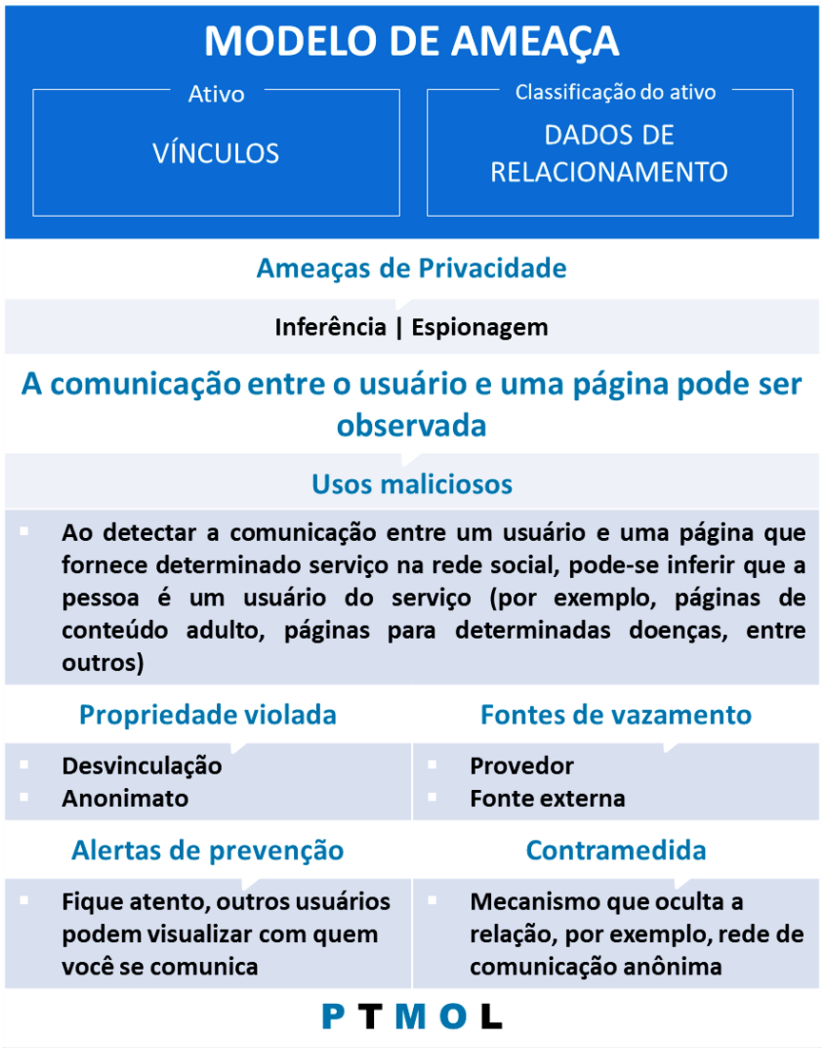


Figura 4.12: Modelo de ameaças da PTMOL
Fonte: Próprio Autor.

Capítulo 5

Avaliação e Evolução da PTMOL por meio de Estudos Empíricos

Este capítulo apresenta o processo de avaliação e evolução da PTMOL com base em resultados de estudos empíricos. O planejamento, execução e resultados dos estudos são apresentados. Foram conduzidos um estudo preliminar, um estudo de viabilidade, um estudo de observação e um estudo com especialistas.

5.1 Introdução

A metodologia de *Design Science Research*, utilizada nesta pesquisa, determina que, na etapa de avaliação, o artefato projetado para solucionar o problema de pesquisa seja rigorosamente avaliado em relação à sua utilidade, qualidade e precisão (Hevner et al., 2004). O pesquisador pode contrastar os resultados obtidos com os objetivos da solução definidos na segunda etapa do DSR. Caso o resultado encontrado não seja o esperado, poderá retornar à etapa de projeto e desenvolvimento do ciclo, a fim de desenvolver um novo artefato.

Para avaliar a linguagem PTMOL como solução para modelagem de ameaças de privacidade no contexto de RSOs, foram conduzidos estudos empíricos em ambiente acadêmico, para coletar oportunidades de refinamento da solução, e um estudo com especialistas, para validar a versão final obtida com os refinamentos realizados. A condução dos estudos permitiu a realização de incrementos na proposta inicial da PTMOL, gerando melhorias e indicadores com relação à sua viabilidade prática. A Figura 5.1 ilustra o processo de avaliação e evolução da PTMOL. Nas próximas seções serão apresentadas as versões da PTMOL e os estudos empíricos conduzidos: estudo preliminar, estudo de viabilidade, estudo de observação e estudo com especialistas. Ressalta-se que o protocolo dos estudos foi aprovado pelo Comitê de Ética e Pesquisa da Universidade Federal do Amazonas (CAAE- 63572122.0.0000.5020).

Com o objetivo de avaliar a versão inicial da PTMOL e compreender seu uso na modelagem de ameaças de privacidade em RSOs, foi realizado um estudo experimental

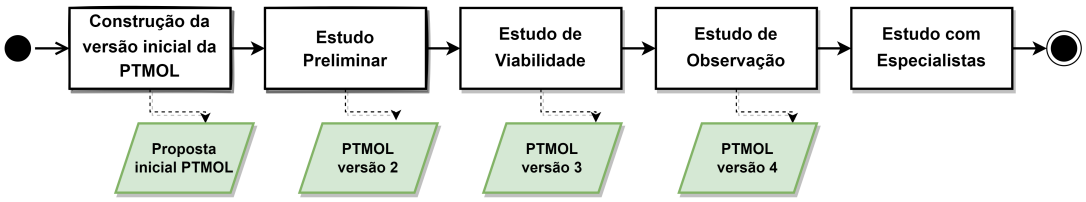


Figura 5.1: Processo de avaliação e evolução da PTMOL
Fonte: Próprio autor.

preliminar (Seção 5.2). O estudo também foi conduzido para realizar os procedimentos de validade e confiabilidade da linguagem e coletar as oportunidades para o seu refinamento.

5.2 Primeiro estudo: validando a versão inicial da PTMOL

Experimentação é o centro do processo científico e oferece o modo sistemático, disciplinado, computável e controlado para avaliação da atividade humana (Travassos et al., 2002). Em diversas áreas da Computação, estudos experimentais são executados com o objetivo de caracterização, avaliação, previsão e melhoria a respeito de processos, métodos, modelos, ferramentas, entre outros. Segundo Shull et al. (2001), a utilização de estudos experimentais, além de prover validação para diferentes propostas, pode também auxiliar na identificação de problemas presentes nas mesmas. A seguir serão descritos o planejamento, execução e resultados obtidos com o estudo experimental preliminar.

5.2.1 Planejamento do Estudo

O design experimental do estudo foi embasado nos trabalhos de Wuyts et al. (2018); Scandariato et al. (2015), que avaliaram técnicas de modelagem. Os conceitos das métricas de corretude, completude e produtividade foram extraídos do trabalho de Wuyts et al. (2018). Com o fundamento nisso, este estudo buscou responder as seguintes questões de pesquisa:

- **QP1 - Corretude**. Em média, quantas ameaças descobertas pelos participantes estão corretas (verdadeiros positivos x falsos positivos)?
- **QP2 - Completude**. Quantas ameaças não são detectadas pelos participantes (falsos negativos)?
- **QP3 - Produtividade**. Quantas ameaças válidas são identificadas pelos participantes em um determinado período de tempo?
- **QP4 - Facilidade de uso**. Os participantes perceberam o modelo como fácil de aprender e aplicar?

- **QP5 - Utilidade**. Os participantes acreditam que o modelo melhoraria seu desempenho no design de ameaças?
- **QP6 - Intenção de uso**. Os participantes utilizariam o modelo em projetos futuros?

A Tabela 5.1 apresenta uma visão geral dos termos adotados para a avaliação quantitativa. A partir das questões de pesquisa supracitadas, foram formuladas hipóteses nulas e alternativas.

Tabela 5.1: Terminologia adotada para a avaliação quantitativa

Termos	**Significado**
Verdadeiro Positivo (VP)	Ameaça correta
Falso Negativo (FN)	Ameaça não identificada
Falso Positivo (FP)	Ameaça incorreta
Precisão (Prec)	VP/(VP+FP)
Recall (Rec)	VP/(VP+FN)
Produtividade (Prod)	VP/tempo
Média (μ)	Média da população

Corretude. Define o quanto um modelo emprega corretamente os elementos e relacionamentos, de acordo com a sintaxe da linguagem. Ao invés de usar o número total de erros cometidos pelos participantes, a corretude foi medida por meio da precisão (Tabela 5.1). A precisão é uma métrica de avaliação que traz a informação da quantidade de observações classificadas como positivas, ou seja, entre todas as observações da classe positivo, quantas foram identificadas corretamente (Olson and Delen, 2008). Por esse ângulo, no contexto deste estudo, a precisão calcula o número de ameaças identificadas corretamente (verdadeiros positivos) em relação aos erros (falsos positivos). Para investigar essa questão de pesquisa, formulou-se uma hipótese nula (H0) conforme descrita na equação abaixo. A hipótese alternativa (expectativa de um bom resultado) defende que a precisão será equivalente ou superior a 80%. O valor de 80% foi embasado em trabalhos relacionados que adotaram o mesmo valor e avaliaram técnicas de modelagem de ameaças em condições experimentais semelhantes (Wuyts et al., 2014; Scandariato et al., 2015).

$$\mathrm{H}_0 : \mu\{\mathrm{Prec} = \frac{VP_{participante}}{VP_{participante} + FP_{participante}}\} < 0.80$$

Completude. Define o quanto a linguagem apresenta um processo de modelagem suficientemente detalhado para auxiliar a identificar um conjunto completo de ameaças. Nesse sentido, a completude foi medida por meio do *recall*. O *recall* é uma métrica que busca identificar a proporção dos verdadeiros positivos entre todas as observações que realmente são positivas. Em outras palavras, representa a capacidade de um modelo prever a classe positiva (Olson and Delen, 2008). Nessa perspectiva, o *recall*, no contexto deste estudo, calculou o número de ameaças identificadas corretamente

(verdadeiros positivos) em relação ao número de ameaças que os participantes não conseguiram identificar (falsos negativos). Com base nisso, a hipótese nula (H0) foi formulada e descrita NA equação abaixo. Assim como na hipótese alternativa anterior, espera-se que o *recall* seja equivalente ou superior a 80%. O valor de 80% também foi embasado nas hipóteses dos estudos de Wuyts et al. (2014).

$$\mathrm{H}_0 : \mu\{\mathrm{Rec} = \frac{VP_{participante}}{VP_{participante} + FN_{participante}}\} < 0.80$$

Produtividade. A produtividade foi definida como o número de ameaças identificadas corretamente (verdadeiros positivos) por hora. Nos trabalhos de Scandariato et al. (2015) e Wuyts et al. (2018) foi observada como uma produtividade média a detecção de uma ameaça por hora. Utilizou-se o mesmo valor adotado nos trabalhos para facilitar uma análise comparativa posterior e porque ambos avaliaram técnicas de modelagem de ameaças com condições experimentais semelhantes. A expectativa é que a PTMOL tenha uma produtividade equivalente ou superior a uma ameaça identificada corretamente por hora. Portanto, a hipótese nula formulada é descrita abaixo.

$$\mathrm{H}_0 : \mu\{\mathrm{Prod} = \frac{VP_{participante}}{tempo}\} < ameaça/hora$$

Para responder as demais questões de pesquisa, utilizou-se um questionário pós-estudo. Esse questionário foi elaborado com base nos indicadores do modelo TAM *(Technology Acceptance Model)*, que tem sido amplamente adotado em diversas pesquisas para avaliar o motivo de usuários aceitarem ou rejeitarem uma determinada solução (Davis, 1989). Os indicadores utilizados como questões de pesquisa foram:

- **Facilidade de uso percebida**. Define o grau no qual uma pessoa considera que utilizar o processo de modelagem de ameaças seria livre de esforço.
- **Utilidade percebida**. Define o grau no qual uma pessoa considera que utilizar o processo de modelagem melhoraria seu desempenho em determinadas atividades de design.
- **Intenção de uso**. Define o grau no qual uma pessoa prevê que utilizaria o processo de modelagem de ameaças no futuro.

5.2.1.1 Participantes

Oito (08) alunos de graduação, do curso de Ciência da Computação da UFAM foram selecionados como participantes do estudo. Esses participantes cursavam a disciplina de Segurança de Sistemas e foram escolhidos por critérios de conveniência. Essa conveniência representa: (i) uma maior facilidade operacional e baixo custo de amostragem; e (ii) os alunos poderiam ter maior conhecimento/consciência sobre ameaças, uma vez que estavam cursando uma disciplina de Segurança de Sistemas.

Os participantes assinaram um Termo de Consentimento Livre e Esclarecido (TCLE) e preencheram um Formulário de Caracterização, para identificar a experiência deles em relação à modelagem de sistemas e privacidade. De acordo com Fernandez et al. (2012), estudantes podem ter habilidades semelhantes aos profissionais menos experientes. Além disso, esses estudantes são pessoas em formação em Computação, portanto, eles dominam o uso de tecnologias e as desenvolvem. Desse modo, os alunos foram caracterizados como projetistas novatos, que estão aprendendo sobre modelagem de ameaças. Com isso, esse estudo tem o potencial de mostrar como esses projetistas, que não conhecem a linguagem de modelagem, fizeram sentido dela e a utilizaram em um contexto de design.

5.2.1.2 Cenário

Para executar uma modelagem de ameaças com a PTMOL, pode-se escolher alguma representação ou modelo utilizado no design de interação com usuário. Para o contexto deste estudo, utilizou-se como base o conceito de design baseado em cenários. Um cenário é "simplesmente uma história sobre pessoas executando uma atividade" (Rosson and Carroll, 2002). As histórias dos cenários estimulam a imaginação da equipe de design e encorajam a análise de caminhos alternativos (Barbosa and Silva, 2010). Para um design de privacidade em RSOs, adaptou-se este conceito e criou-se o design baseado em cenários de ameaças. Escolhemos essa técnica pois, ao ler e revisar um potencial cenário de ameaças, a equipe de design tem a oportunidade de discutir e analisar como as atividades de compartilhamento e coleta de dados dos usuários poderiam ser afetadas por usos indevidos e maliciosos, que podem comprometer a sua privacidade.

Nesse sentido, o cenário utilizado descrevia uma potencial interação, via chat, entre dois usuários de uma RSO. No geral, o cenário mostrava uma usuária procurando perfis na RSO que ofereciam serviços de reparos residenciais com atendimento rápido e fácil. A usuária encontra um perfil e envia uma mensagem, via chat, para saber mais informações sobre os serviços prestados. No entanto, aquela página é gerenciada por um agente malicioso, que tenta descobrir dados pessoais da vítima. O cenário não descrevia as ameaças de privacidade que poderiam ocorrer, pois o objetivo era observar se os elementos da PTMOL direcionariam os participantes a modelarem as ameaças de privacidade presentes no cenário.

Cabe salientar que, antes da execução do estudo, foi realizada uma modelagem com a PTMOL, pelo autor da pesquisa, em relação ao cenário fornecido, e posteriormente essa análise foi revisada e consolidada por outros dois pesquisadores. A partir disso, criou-se um oráculo (solução de referência) contendo todas as possíveis ameaças que uma modelagem ideal com a PTMOL produziria (Apêndice F). Esse oráculo foi utilizado para verificar se os participantes desconsideraram ou não identificaram algumas ameaças (falsos negativos) presentes no cenário referido. No total, dezesseis (16) ameaças de privacidade poderiam ocorrer dependendo da forma de compartilhamento dos ativos. Esse valor é a referência para a análise da completude e corretude.

5.2.1.3 Instrumentação

Diversos instrumentos foram definidos para apoiar o estudo, tais como: (i) Termo de Consentimento Livre e Esclarecido (TCLE); (ii) formulário de caracterização do perfil dos participantes; (iii) cenário de ameaça; (iv) roteiro de tarefas; (v) material de apoio para a aplicação da PTMOL; e (vi) questionário pós-estudo (Apêndice C).

5.2.1.4 Tarefas

Os participantes deveriam empregar a linguagem PTMOL para o cenário fornecido, realizando as seguintes tarefas: (i) identificar os ativos; (ii) identificar as ameaças; (iii) identificar as ações do atacante; (iv) identificar estratégias de mitigação; e (v) gerar o modelo de ameaças.

5.2.2 Execução do primeiro estudo

O estudo foi executado remotamente devido o cenário atual de pandemia. A execução remota não influenciou a condução do estudo, uma vez que todas as tarefas planejadas foram realizadas corretamente pelos participantes. A execução do estudo foi dividida em três etapas: preparação, aplicação e avaliação. Tais etapas foram conduzidas por um pesquisador (autor do modelo) e serão descritas em detalhes a seguir.

5.2.2.1 Preparação

Nesta etapa, os participantes receberam as informações pertinentes quanto à execução da modelagem de ameaças de privacidade. O autor da pesquisa apresentou aos participantes um tutorial prático síncrono, de aproximadamente 1 hora, contendo uma breve introdução aos principais conceitos de privacidade em RSOs e uma explicação detalhada sobre a aplicação do processo de modelagem da PTMOL a um eventual cenário de ameaças.

5.2.2.2 Aplicação

Após a preparação, os participantes aplicaram a PTMOL para modelar ameaças de privacidade de acordo com o cenário fornecido. No início desta etapa, o pesquisador responsável disponibilizou o TCLE e o formulário de caracterização do perfil. Em seguida, o pesquisador disponibilizou o roteiro de tarefas e o material de apoio, explicando o que continha cada artefato. O roteiro de tarefas descrevia explicitamente as diferentes etapas do modelo que os participantes deveriam executar. Como material de apoio, eles receberam a tabela de registro de ameaças e o tutorial de aplicação do modelo.

O pesquisador atuou como instrutor durante a condução do estudo, sendo o principal responsável por auxiliar em casos de dúvidas referentes ao processo de modelagem, tomando a devida precaução para não influenciar na execução das tarefas. O pesquisador informou aos participantes ainda que, após a conclusão das tarefas, um questionário deveria ser respondido para reportar a experiência de uso com a linguagem.

Não foi definido um limite de tempo para a realização das tarefas, ou seja, os participantes puderam realizar as atividades de modelagem livremente, desde que registrassem o tempo inicial e o tempo final gasto no processo de modelagem. Todos os participantes entregaram as suas tabelas, que documentavam detalhadamente a análise realizada, o tempo gasto e o modelo de ameaças gerado.

5.2.2.3 Avaliação

Por fim, os participantes foram solicitados a fornecer um *feedback*, por meio de um questionário pós-estudo, sobre a sua experiência de uso com a PTMOL. Com isso, buscou-se coletar indicadores quantitativos e reflexões qualitativas para ganhar novos *insights* quanto à aplicação prática da linguagem. Buscou-se também, a partir dessa avaliação, obter indicadores sobre as possibilidades e/ou dificuldades em compreender o que é modelar ameaças de privacidade no contexto de RSOs, bem como obter oportunidades para o refinamento da linguagem.

5.2.3 Resultados do primeiro estudo

Após a execução e conclusão do estudo, os artefatos gerados pelos participantes (tabelas de registro de ameaças e modelos), bem como os dados coletados pelos questionários pós-estudo, foram analisados. Nesta seção, os resultados quantitativos e qualitativos obtidos serão apresentados e discutidos.

5.2.3.1 Resultados quantitativos

O cenário fornecido reportava seis ativos sendo compartilhados via chat pela vítima, a saber: nome, telefone, endereço de e-mail, fotos, vídeos e endereço residencial. Dependendo da forma de compartilhamento do ativo, diferentes ameaças de privacidade poderiam ocorrer. Os relatórios gerados pelos participantes foram avaliados por especialistas (autores do modelo). Cada ameaça reportada na tabela de registro foi avaliada como correta (verdadeiro positivo) ou incorreta (falso positivo). Os resultados corretos são ameaças consideradas: a) relevantes para o contexto do cenário fornecido; b) compatíveis com as ameaças consideradas pela linguagem PTMOL; e c) documentadas com detalhes e raciocínio suficientes.

A Tabela 5.2 apresenta uma visão geral dos resultados quantitativos obtidos a partir da análise individual sobre a modelagem realizada pelos participantes. O rótulo 'P', seguido de um número, indica cada participante, por exemplo, P1 identifica o participante 1 e assim sucessivamente.

Completude e Corretude (QP1-QP2). A corretude foi calculada por meio da precisão, que analisa a taxa de ameaças identificadas corretamente (verdadeiros positivos) em relação ao número de ameaças incorretas (falsos positivos). Já a completude foi medida por meio do *recall*, que calcula o número de ameaças identificadas corretamente (verdadeiros positivos) em relação ao número de ameaças não detectadas (falsos

Tabela 5.2: Resultados quantitativos da modelagem realizada pelos participantes

Termos	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**
Ameaças encontradas	12	9	16	10	11	10	11	8
Verdadeiros positivos	9	9	11	10	8	9	9	7
Falsos positivos	3	0	5	0	3	1	2	1
Falsos negativos	7	7	5	6	8	7	7	9
Tempo gasto (horas)	2,21	1,04	1,22	1,46	1,38	1,58	1,35	1,32
Precisão	75%	100%	69%	100%	73%	90%	82%	88%
Recall	56%	56%	69%	63%	50%	56%	56%	44%
Produtividade	4	9	9	7	6	6	7	5

negativos). A Tabela 5.3 apresenta os resultados quantitativos para os indicadores de Corretude e Completude.

Tabela 5.3: Resultados quantitativos da Corretude e Completude

#P	**Corretude(%)**	**Completude(%)**
P1	75,00%	56,25%
P2	100,00%	56,25%
P3	68,75%	68,75%
P4	100,00%	62,50%
P5	72,73%	50,00%
P6	90,00%	56,25%
P7	81,82%	56,25%
P8	87,50%	43,75%
Média	**84,47%**	**56,25%**

Foi obtida uma média acima de 0,80 para corretude, sugerindo um resultado positivo para este indicador e retendo a hipótese nula (H0). Esse resultado demonstra que a linguagem PTMOL possui uma boa corretude e ajuda a identificar ameaças válidas no design de privacidade em RSOs. Em relação a completude, nota-se que a taxa do *recall* foi de 0,562, abaixo da expectativa. Tal resultado apoia a hipótese nula (0,80 em H0). Além disso, esse resultado também pode ser analisado observando os dados da Tabela 5.2, onde é possível notar a incidência de falsos negativos. Isso indica que pode ter ocorrido dificuldades na representação de alguns elementos da PTMOL ou o participante não entendeu corretamente a semântica da linguagem, fazendo com que algumas ameaças presentes no cenário fornecido não fossem detectadas. Essa análise validou a corretude do modelo e demonstrou que necessidades de melhorias precisavam ser feitas para aprimorar a sua completude.

Produtividade. 0s participantes gastaram um total de 11 horas na modelagem de ameaças, o que resulta em uma produtividade de 1,33 ameaça por hora. A expectativa seria que a PTMOL tivesse uma produtividade equivalente ou superior a uma ameaça identificada corretamente por hora. Com isso, é possível observar que a linguagem obteve uma boa produtividade na sua execução, rejeitando a hipótese nula.

5.2.3.2 Análise da percepção dos participantes sobre a PTMOL

Os participantes forneceram suas percepções em relação à linguagem de modelagem de ameaças por meio de um questionário pós-estudo. Para coletar os dados qualitativos, foi aplicada uma escala ordinal de seis pontos variando em: (6) *concordo totalmente*; (5) *concordo amplamente*; (4) *concordo parcialmente*; (3) *discordo parcialmente*; (2) *discordo amplamente*; e (1) *discordo totalmente*. Conforme sugerido por Laitenberger and Dreyer (1998), o ponto neutro *(nem concordo, nem discordo)* não foi utilizado na escala ordinal, uma vez que não permite identificar a inclinação (positiva ou negativa) das respostas dos participantes.

Facilidade de uso percebida. Define o grau no qual uma pessoa considera que utilizar o processo de modelagem de ameaças seria livre de esforço. Para coletar esse indicador, foram definidas as seguintes afirmações com as quais os participantes deveriam expressar seu grau de concordância: (F1) Aprender a modelar ameaças de privacidade com esta linguagem foi fácil para mim; (F2) Eu achei fácil de utilizar esta linguagem como eu gostaria (os elementos da linguagem são claros e compreensíveis); (F3) Eu entendia o que acontecia enquanto utilizada esta linguagem; e (F4) Eu considero esta linguagem fácil de usar. A Figura 5.2 apresenta uma representação gráfica sobre a percepção dos participantes em relação ao indicador facilidade de uso.

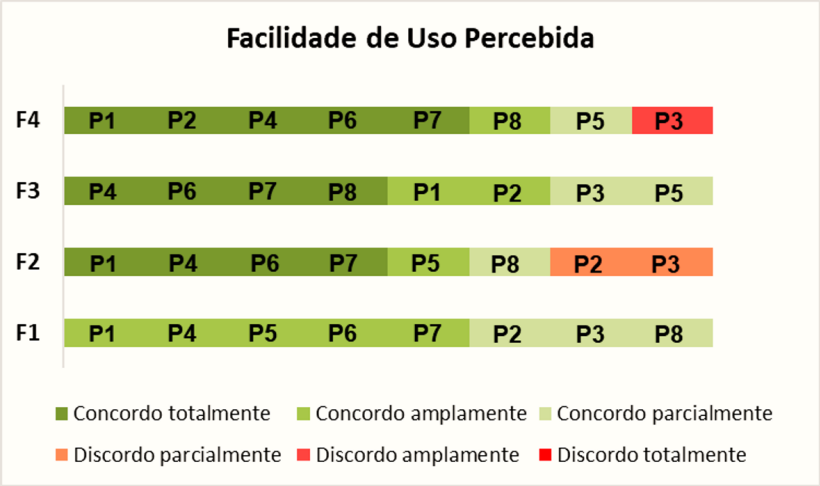


Figura 5.2: Percepção sobre a Facilidade de Uso da PTMOL

Analisando os dados fornecidos pela Figura 5.2, é possível observar que os participantes P2 e P3 discordaram parcialmente em relação à afirmativa F2. Esse grau de discordância pode ser um indicador de que a linguagem ainda não estava totalmente clara e compreensível. Além disso, esse dado também pode justificar o grau de completude apresentado na Tabela 5.3, demonstrando que a linguagem pode melhorar sua semântica para apresentar informações mais suficientes de acordo com o propósito da modelagem de ameaças.

Em relação à afirmativa (F1) *"Aprender a modelar ameaças de privacidade com esta linguagem foi fácil para mim"*, observa-se que não houveram incidências de discordâncias. Tais respostas indicam um resultado positivo para a PTMOL, demonstrando que a linguagem tem uma boa facilidade de aprendizado. Além disso, um outro resultado relevante a ser destacado é a não ocorrência de discordância quanto à afirmativa F3 "*Eu entendia o que acontecia enquanto utilizada esta linguagem*". Esse resultado sugere que o entendimento sobre o processo de modelagem de ameaças da PTMOL tem uma facilidade pertinente.

Utilidade percebida. Define o grau no qual uma pessoa considera que utilizar o processo de modelagem de ameaças melhoraria seu desempenho em determinadas atividades de design. Para coletar a utilidade percebida, foram definidas as seguintes afirmativas: (U1) Usar esta linguagem me torna capaz de modelar ameaças de privacidade em RSOs rapidamente; (U2) Usar esta linguagem torna o meu desempenho melhor na modelagem de ameaças de privacidade de RSOs; (U3) Usar esta linguagem poderá melhorar a minha produtividade na modelagem de ameaças de privacidade em RSOs, pois acredito que identificaria um número maior de ameaças em um tempo menor do que identificaria sem utilizá-la; e (U4) Eu considero que esta linguagem é útil para apoiar o processo de modelagem de ameaças de privacidade em RSOs. A Figura 5.3 detalha os resultados sobre a utilidade percebida.

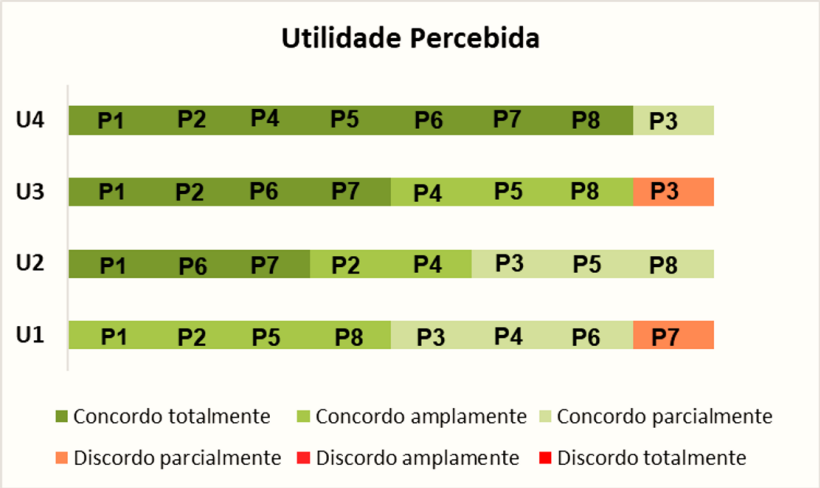


Figura 5.3: Percepção sobre a Utilidade da PTMOL

Com base na Figura 5.3, nota-se que a maioria dos participantes concordaram com as afirmativas em relação à utilidade, indicando que eles acreditam que PTMOL melhoraria o desempenho e aumentaria a produtividade na modelagem de ameaças de privacidade em RSOs. Ou seja, eles concordaram que, com o apoio da linguagem, é possível identificar um número maior de ameaças, em um tempo menor do que identificariam sem utilizá-la. Portanto, no contexto desse estudo, a PTMOL obteve um resultado positivo quanto à sua utilidade.

Intenção de uso. Define o grau no qual uma pessoa prevê que utilizaria o processo de modelagem de ameaças no futuro. Para coletar a intenção de uso sobre a linguagem, utilizou-se as seguintes questões: (I1) Supondo que eu tenho tempo suficiente para modelar ameaças de privacidade em RSOs, eu utilizaria esta linguagem; (I2) Levando em conta que eu tenho domínio para escolher qualquer suporte para a modelagem de ameaças de privacidade em RSOs, eu prevejo que eu irei usar esta linguagem; e (I3) Eu pretendo usar esta linguagem em outros momentos. A Figura 5.4 apresenta as respostas dos participantes sobre a intenção de utilizar a PTMOL futuramente.

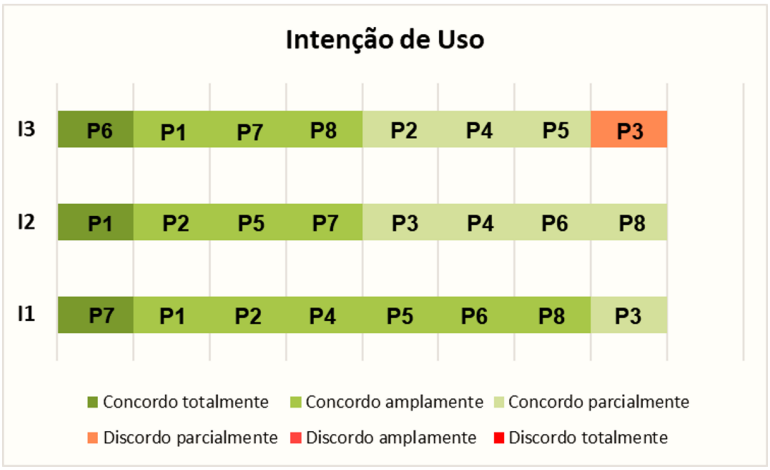


Figura 5.4: Percepção sobre Intenção de Uso da PTMOL

Foram obtidos resultados positivos em relação a este indicador. O fato dos participantes terem experiência acadêmica com outros modelos de análise e projeto fortalece o resultado da afirmativa I2, que ressalta a preferência em utilizar a PTMOL. Esses resultados sugerem que os participantes teriam a intenção de usar a linguagem PTMOL futuramente em atividades de design de privacidade.

5.2.3.3 Resultados Qualitativos

Uma análise específica com relação aos comentários dos participantes (dados qualitativos), obtidos por meio de perguntas abertas contidas no questionário pós-estudo, foi realizada. As respostas às questões abertas permitiram analisar mais profundamente os resultados obtidos. Todos os participantes forneceram feedbacks importantes sobre o processo de modelagem da PTMOL.

Os comentários fornecidos pelos participantes em relação aos aspectos positivos da linguagem indicam citações que constatam a facilidade de aprendizado da PTMOL. O participante P3 afirmou: "*O guideline explicando o que significa cada elemento é bem intuitivo e fácil de entender, além (da linguagem) cobrir boa parte das ameaças de privacidade que podem ocorrer em RSOs*". Outros comentários enfatizaram a importância da reflexão que a linguagem proporciona quanto à proteção dos ativos compartilhados pelo usuário, bem como a sua relevância para o tratamento de ameaças desde o design:

o participante P2 destacou: "*O modelo é bem interessante e trouxe uma visão sobre os ativos e como evitar e tratar as ameaças de uma forma bem significativa*".

Como aspectos negativos, alguns participantes salientaram o tempo de esforço que o processo de modelagem com a PTMOL pode demandar. O participante P1 relatou: "*O ponto negativo é o tempo, dependendo do tamanho e do contexto da aplicação, a utilização da linguagem pode demandar bastante tempo*". Outro participante destacou (P6): *"Demanda um pouco mais de tempo e de criatividade para descrever as ações do atacante"*. Isso pode ser um indicador de que a PTMOL exige um tempo de esforço para conduzir a modelagem de ameaças de privacidade. No entanto, melhorias podem ser realizadas para que ela exija menos esforço em tempo de uso.

Algumas dificuldades com relação ao processo metodológico da PTMOL foram identificadas com base nas respostas fornecidas pelos participantes do estudo. As principais dificuldades coletadas foram as seguintes: uma dificuldade da PTMOL é que ela é um pouco dispendiosa: *"Acho uma boa técnica que permite pensar nas ameaças, mas demanda um pouco mais de tempo e criatividade para as ações do atacante"* - (P4); alguns elementos da PTMOL têm o mesmo conceito: *"Os elementos de controle e contramedida tendem a causar confusão conceitual em um primeiro momento, indicando falta de clareza entre os conceitos "* - (P1) e *"Não entendi muito bem a diferença entre controle e contramedida, da forma como é descrito parecem ser a mesma coisa*" - (P8); alguns conceitos de ameaças do catálogo precisam ser reformulados: "*Acho que seria interessante os autores reverem alguns conceitos das ameaças do catálogo porque algumas podem estar se confundindo, ou até mesmo deixar mais claro para quem vai aplicá-las*" - (P3).

Outras dificuldades apontadas pelos participantes eram relacionadas à manipulação da tabela de registro de ameaças, recurso da linguagem para que os projetistas possam documentar sua análise e posteriormente gerar o modelo de ameaças. O participante P2 relatou: "*Tive dificuldade com o uso de um dos recursos da modelagem, a tabela para reportar ameaças*". Outro participante (P4) destacou "*Tive dificuldade somente com a manipulação das tabelas (de registro de ameaças), pois eram várias e bem parecidas às vezes, alterando só uma coluna, o que causou um retrabalho*".

Outro problema relatado quanto à dificuldade de aplicação estava relacionado à transferência das informações da tabela de registro para o modelo. O participante P1 destacou que algumas informações descritas de forma detalhada na tabela ficavam difíceis de representar no modelo: "*Outro problema foi quanto à transposição das tabelas da modelagem para o modelo, onde estava disposta alguma informação genérica mas não especifica o suficiente para servir de rótulos para os elementos no modelo - seria bom ter tido uma ideia desse aspecto do modelo já do início da modelagem*". Esse relato pode servir como sugestão de melhoria para o modelo, onde alguma estratégia pode ser considerada para resumir informações detalhadas no momento da transposição para o modelo.

5.2.4 Melhorias na PTMOL

Esta seção fornece uma visão geral das melhorias implementadas no processo de modelagem da PTMOL. A partir das análises realizadas nos questionários pós-estudo, foi possível entender alguns pontos que causaram certas dificuldades durante a aplicação da linguagem. Esses pontos geraram reflexões de que alguns elementos da PTMOL não estavam claros e compreensíveis. Para cada uma das dificuldades coletadas, uma mudança no processo metodológico da PTMOL foi sugerida, conforme mostrado na Tabela 5.4. Essas melhorias baseadas em evidências são discutidas nas seções a seguir.

Tabela 5.4: Principais problemas da PTMOL e melhorias sugeridas

Problema	**Fonte**	**Melhorias na PTMOL**
1. **Elementos com definições semelhantes**		
Controle e Contramedida	Feedback dos participantes	Remoção do elemento controle
2. **Recursos e elementos confusos**		
	Feedback + Observação	Reestruturação dos elementos
3. **Baixo valor na taxa de completude**		
	Resultados (FN)	Ampliação de elementos
4. **Catálogo de ameaças com poucos detalhes**		
	Feedback + Observação + Resultados (FN e FP)	Ampliação e reestruturação do catálogo

5.2.4.1 Elementos com definições semelhantes

Os comentários feitos pelos participantes do estudo indicaram que a relação entre alguns elementos da PTMOL precisava ser revisada para evitar redundâncias. Entre os elementos citados, estavam o "controle" e a "contramedida", os quais foram apontados e percebidos com o mesmo significado. Ao revisar esses componentes da PTMOL, observou-se que o elemento "controle" também é uma forma de contramedida para prevenir ou neutralizar uma ameaça. Portanto, a finalidade do elemento está fortemente ligada ao propósito da contramedida. Com isso, optou-se por retirar o elemento "controle" da composição de elementos da PTMOL e deixar somente os elementos "alerta de prevenção" e "contramedidas" como estratégias de mitigação.

5.2.4.2 Recursos e elementos confusos

Durante o estudo, observou-se diversas dúvidas relacionados a alguns recursos e elementos da PTMOL, pois, no geral, alguns eram confusos ou difíceis de compreender. Essa questão indicou oportunidades de refinamento e inspirou a realização de algumas mudanças para melhorar a compreensão e a navegabilidade entre os componentes da linguagem.

O elemento “ações do atacante”, que permitia o designer criar um raciocínio sobre as possíveis ações que um agente malicioso pode realizar quando estiver de posse dos ativos do usuário, foi renomeado. Para deixar mais claro o propósito do componente da PTMOL, o nome do elemento foi alterado para “usos maliciosos”, que tenta prever qual comportamento indevido ou malicioso o atacante pode executar ao obter acesso aos dados privados do usuário. A Figura 5.5 ilustra esse incrimento realizado na nomenclatura do elemento.

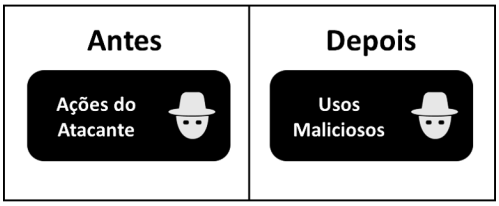


Figura 5.5: Atualização do elemento da PTMOL
Fonte: Próprio autor.

Outro ponto observado em relação ao procedimento metodológico da PTMOL refere-se à etapa de identificação de ativos. Nessa etapa, o designer deve identificar os ativos a serem protegidos, antes de começar a descobrir quais ameaças podem ocorrer. Dependendo da forma como o ativo foi compartilhado no sistema, três formas de compartilhamento, e suas respectivas variantes, são definidas para possibilitar uma classificação do ativo. No entanto, observou-se que, o *template* para classificação de ativos é destinado somente para ativos compartilhados pelo usuário no sistema. Esse *template* não previa a classificação dos ativos coletados e processados pelo sistema, que não necessariamente são compartilhados pelo usuário, mas que são coletados e combinados para gerar outras informações pessoais. Esses ativos referem-se a: (i) dados de uso; e (ii) dados de relação. Com isso, criou-se um segundo *template* para também viabilizar a classificação de ativos coletados pelo sistema, conforme ilustrado na Figura 5.6.

Ativos	ATIVOS COLETADOS PELO SISTEMA	
	Dados de uso	Dados de relacionamento
Ativo 1		
Ativo 2		
Ativo 3		
...		
Ativo n		
<Listar todos os ativos>	<Marcar com “X” se o ativo pertencer a essa categoria>	<Marcar com “X” se o ativo pertencer a essa categoria>

Figura 5.6: Novo *template* para classificação de ativos coletados pelo sistema
Fonte: Próprio autor.

5.2.4.3 Baixo valor na taxa de Completude

Os resultados do estudo preliminar mostraram um nível relativamente baixo relacionado à métrica de completude. Ao examinar as perguntas feitas pelos participantes durante a pesquisa, bem como alguns comentários coletados no questionário pós-estudo, percebeu-se que alguns elementos da PTMOL estavam confusos e outros estavam ausentes, como, por exemplo, a tabela para classificação de ativos coletados pelo sistema. Tais componentes são um suporte importante para alcançar a completude. Isso implica que a ausência de recursos importantes no procedimento metodológico da PTMOL impactou a sua completude no primeiro estudo. No entanto, conforme mostrado anteriormente, mudanças e incrementos foram realizados de modo a possibilitar uma modelagem de ameaças de privacidade mais completa para o contexto de RSOs.

5.2.4.4 Catálogo de ameaças com poucos detalhes

Durante o estudo, alguns participantes indicaram que o catálogo de ameaças estava com poucos detalhes. De fato, o catálogo poderia se beneficiar de uma descrição mais aprimorada de cada ameaça. Além disso, algumas observações durante o estudo mostraram que o conhecimento geral dos participantes sobre as categorias de ameaças era bastante limitado.

A partir disso, criou-se uma descrição geral para cada tipo de ameaça da PTMOL pois, durante os estudos, percebeu-se que nem sempre os participantes estavam familiarizados com os conceitos generalistas de um tipo específico de ameaça. A Figura 5.7 mostra um exemplo desse refinamento para o catálogo de ameaças. Vale ressaltar que a intenção não é fornecer uma visão completa do tipo de ameaça, mas sim resumir os conceitos-chave. Um resumo de cada categoria de ameaça foi organizado levando em consideração dois itens principais:

- **Descrição geral**. Esta descrição resume os principais conceitos do tipo de ameaça de privacidade.
- **Impactos**. Resume os possíveis impactos de tais ameaças para a privacidade do usuário. Esse resumo ajudará a entender a gravidade da ameaça. Em outras palavras, a ameaça em si não parece ter um grande impacto, no entanto, suas consequências podem ser bastante invasivas com relação à privacidade (por exemplo, capacidade de vinculação).

5.2.5 Limitações do primeiro estudo

Em todo estudo existem limitações que podem afetar a sua validade. Esse estudo é relativamente pequeno em termos de amostra (oito participantes). Portanto, nenhuma significância estatística forte é esperada e os resultados quantitativos devem ser considerados exploratórios.

Outra limitação é o fato de os participantes serem estudantes de graduação e o estudo ser conduzido em um ambiente acadêmico. No entanto, estudantes podem

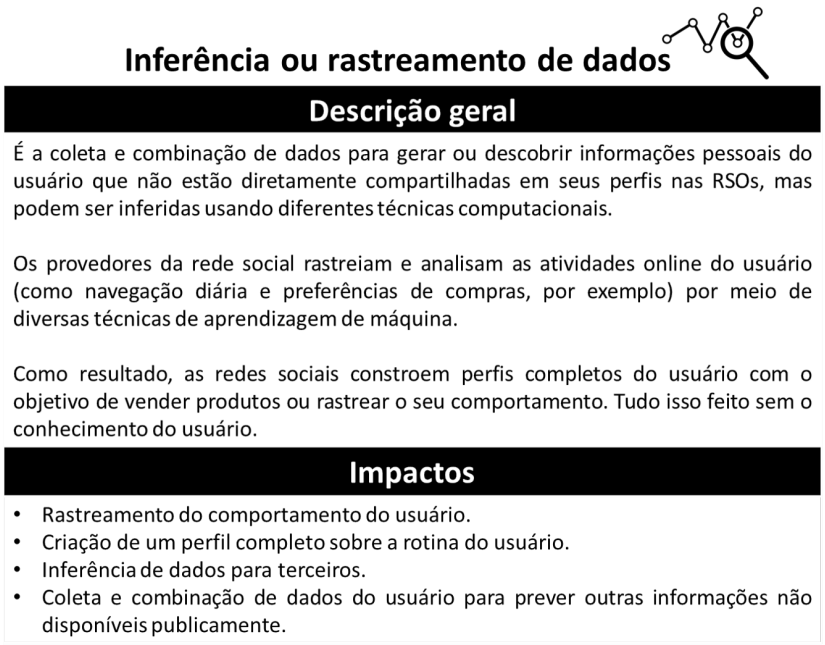


Figura 5.7: Exemplo da descrição geral da ameaça aprimorada: Inferência ou rastreamento de dados

Fonte: Próprio autor.

ter habilidades semelhantes a profissionais menos experientes (Fernandez et al., 2012). Dessa forma, os participantes são considerados designers prospectivos e executaram a modelagem de um eventual cenário de ameaça ao qual um usuário estaria potencialmente exposto. Além disso, a PTMOL também é voltada para projetistas novatos. Portanto, a amostra reflete a população do estudo.

5.2.6 Conclusões do primeiro estudo

Esta seção apresentou o planejamento, execução e resultados de um estudo preliminar realizado com a linguagem PTMOL. Os resultados quantitativos apontaram que a solução tem uma boa corretude e foi considerada útil e fácil de aplicar. Além disso, os resultados quantitativos também indicaram que eram necessárias melhorias no indicador de completude da solução. Os participantes apontaram dúvidas no uso da notação e no entendimento da PTMOL, fato que levou à incidência de incompletude. Assim, melhorias foram implementadas de modo a possibilitar um procedimento metodológico mais completo.

Os dados qualitativos obtidos por meio dos questionários pós-estudo demonstraram que, de um modo geral, os participantes consideraram que a PTMOL apoia o processo de modelagem de ameaças. Embora dois participantes tenham indicado discordância em relação às afirmativas que avaliaram a clareza e compreensão da linguagem, a PTMOL, no geral, foi considerada fácil de aprender e aplicar. Além disso, por

meio da análise qualitativa, foram também identificadas melhorias a serem realizadas no processo de aplicação, como a necessidade de inserção ou adaptação de elementos que permitam tornar o processo de modelagem de ameaças efetivamente mais claro. Com base nos comentários dos participantes, a PTMOL foi refinada para atender às necessidades de melhorias identificadas e uma nova versão da linguagem foi criada.

Portanto, neste primeiro estudo, os resultados obtidos possibilitaram realizar os procedimentos de avaliação de validade da proposta e coletar as oportunidades para o seu refinamento. Com o objetivo de avaliar viabilidade prática da segunda versão da notação da PTMOL, foi conduzido um estudo de viabilidade, descrito na seção seguinte.

5.3 Segundo estudo: avaliando a viabilidade prática da PTMOL

Estudos experimentais devem ser realizados e repetidos para melhorar a qualidade da proposta que está sendo desenvolvida, tornando público a outros pesquisadores o conhecimento utilizado na execução do experimento e possibilitando uma melhor compreensão e análise da proposta (Basili, 1996). Com o objetivo de obter novos dados para aprimorar o contexto de uso da PTMOL, realizou-se um estudo de viabilidade.

No contexto da condução de estudos experimentais, o estudo de viabilidade é um dos primeiros estudos a ser conduzido para avaliar uma solução recém-criada e verificar sua viabilidade mediante o objetivo proposto (Travassos et al., 2002). Um estudo de viabilidade não pretende obter uma resposta concreta e definitiva, mas sim capturar dados para refinar a solução que está sendo testada e gerar hipóteses sobre o seu uso. Nesse sentido, o propósito deste estudo de viabilidade foi responder a seguinte questão: "*A linguagem PTMOL é viável em relação ao número de ameaças encontradas*"? Este estudo avalia a viabilidade da PTMOL como uma linguagem para a modelagem de ameaças de privacidade em nível de design. O estudo analisa os resultados da aplicação da PTMOL por um conjunto de participantes de um curso de Ciência da Computação. A seguir serão apresentados o planejamento, execução e resultados obtidos no estudo.

5.3.1 Planejamento

O estudo foi planejado para ser executado em dois dias. No primeiro dia, os participantes receberam um treinamento inicial sobre a linguagem. Já no segundo dia, os participantes realizaram a aplicação da PTMOL em um cenário de ameaças. O planejamento detalhado do estudo será descrito nas próximas subseções.

5.3.1.1 Participantes

Doze (12) participantes do curso de Ciência da Computação de uma instituição de ensino superior foram selecionados. Esses participantes cursavam a disciplina de Segurança de Sistemas Computacionais e foram escolhidos por critérios de conveniência.

Ressalta-se que nenhum dos participantes desse estudo tinham participado do estudo anterior.

A fim de assegurar o consentimento voluntário dos participantes no estudo e respeitar os aspectos éticos, eles autorizaram a participação na pesquisa por meio de um Termo de Consentimento Livre e Esclarecido – TCLE. Os participantes foram informados que tinham a plena liberdade de retirar o seu consentimento, em qualquer fase da pesquisa, sem penalização alguma. Adicionalmente, os participantes deveriam preencher um formulário de caracterização para identificar a experiência deles em modelagem de sistemas e privacidade. O conhecimento prévio dos participantes em relação a modelagem de sistemas foi classificado como: (i) sim, se os participantes já haviam realizado atividades de modelagem em disciplinas de graduação, em uma pesquisa ou em empresas de software; e (ii) não, se os participantes nunca realizaram atividades de modelagem. Em relação à experiência dos participantes sobre privacidade, considerou-se com:

- Alta experiência (A): participantes que tinham participado em mais de 5 projetos de privacidade na indústria;
- Média Experiência (M): participantes que tinham participado entre 1 e 4 projetos de privacidade na indústria;
- Baixa Experiência (B): participantes que participaram em pelo menos um projeto de privacidade em sala de aula.
- Nenhuma Experiência (N): participantes que não tinham conhecimento sobre privacidade ou que conheciam apenas alguns conceitos de privacidade adquiridos em leituras/palestras, mas sem nenhuma experiência prática.

Após finalizar o processo de aplicação da PTMOL, os participantes responderam um questionário pós-estudo para relatarem suas experiências durante as atividades de modelagem com a linguagem. Posteriormente à coleta de dados, os participantes foram informados que poderiam ainda solicitar a exclusão do conteúdo fornecido nos questionários, de forma integral ou parcial. Nenhum participante solicitou essa questão.

5.3.1.2 Cenário

Assim como no estudo anterior, a pesquisa foi direcionada a um design baseado em cenários de ameaças. O cenário utilizado para o contexto desse estudo descrevia uma potencial interação de um usuário que se conectava pela primeira vez em uma RSO de compartilhamento de conteúdo. Em linhas gerais, o cenário demonstrava um usuário formando um perfil com algumas informações pessoais que ficariam disponíveis publicamente. Além disso, o usuário também disponibilizava uma foto em seu perfil e divulgava um vídeo com uma legenda que informava que o mesmo estava indo para uma viagem. No vídeo, o usuário também divulgava a sua localização atual. Por fim, o usuário realizava uma compra no sistema fornecendo alguns dados do seu cartão. Nesse

cenário, não foram descritas explicitamente as ameaças de privacidade que poderiam ocorrer, pois o objetivo era observar se processo metodológico da PTMOL direcionaria os participantes a diagnosticarem as ameaças de privacidade presentes no cenário.

5.3.1.3 Instrumentos

Como no estudo anterior, alguns instrumentos importantes foram utilizados para apoiar a condução do estudo e a coleta de dados, tais como: (i) Termo de Consentimento Livre e Esclarecido (TCLE); (ii) formulário de caracterização do perfil dos participantes; (iii) cenário de ameaça; (iv) roteiro de tarefas; (v) material de apoio para a aplicação do PTMOL; e (vi) questionário pós-estudo (Apêndice C).

5.3.1.4 Tarefas

Os participantes receberam um roteiro de tarefas que descrevia as etapas do processo de modelagem de ameaças da PTMOL, as quais eles deveriam executar. Seguindo as etapas do processo, os participantes deveriam: (i) identificar os ativos; (ii) identificar as ameaças; (iii) identificar os usos maliciosos; (iv) identificar estratégias de mitigação; e (v) gerar o modelo de ameaças para o cenário fornecido.

5.3.1.5 Hipóteses

Com base na questão de pesquisa descrita na Seção 5.3, foram formuladas as seguintes hipóteses nulas (H01, H02 e H03) e hipóteses alternativas (HA1, HA2 e HA3) correspondentes:

- **Corretude**. O primeiro conjunto de hipóteses refere-se a corretude, que define o quanto a linguagem emprega corretamente os seus elementos de acordo com a sintaxe estabelecida. Ao invés de usar o número total de erros praticados pelos participantes, a corretude foi medida por meio da precisão. Nesse sentido, formulou-se as hipóteses nula e alternativa descritas abaixo:
  - H01: Não há diferença entre o número de ameaças identificadas corretamente (verdadeiros positivos) em relação ao número de ameaças incorretas (falsos positivos).
  - HA1: O número de ameaças identificadas corretamente (verdadeiros positivos) é maior que o número de ameaças incorretas (falsos positivos).
- **Completude**. O segundo conjunto de hipóteses refere-se a completude, que define o quanto a linguagem apresenta um processo de modelagem suficientemente detalhado para auxiliar a identificar um conjunto completo de ameaças. A completude foi medida por meio do *recall*. A hipótese nula e alternativa são descritas a seguir:

  - H02: Não há diferença entre o número de ameaças identificadas corretamente (verdadeiros positivos) em relação ao número de ameaças não detectadas (falsos negativos).
  - HA2: O número de ameaças identificadas corretamente (verdadeiros positivos) é maior que o número de ameaças não detectadas (falsos negativos).

- **Produtividade**. O terceiro conjunto de hipóteses refere-se à produtividade, que avalia quantas ameaças válidas são identificadas pelos participantes em um determinado período de tempo. A produtividade é definida como o número de ameaças corretas (VP) por hora. As hipóteses nula e alternativa estão descritas abaixo:

  - H03: A produtividade do processo de modelagem de ameaças que aplica a PTMOL é inferior a uma ameaça por hora.
  - HA3: A produtividade do processo de modelagem de ameaças que aplica a PTMOL é maior ou igual a uma ameaça por hora.

5.3.1.6 Preparação dos participantes

O estudo foi planejado para ser executado em dois dias. No primeiro dia, os participantes receberam um treinamento sobre a linguagem e no segundo dia eles realizaram a aplicação da PTMOL ao cenário de ameaças fornecido. O treinamento com os participantes foi dividido em duas etapas com duração de uma hora cada. Durante a primeira etapa, foi introduzido conceitos gerais sobre ameaças e violações de privacidade em RSOs e uma apresentação especificada da linguagem PTMOL. Na segunda etapa, foi demonstrado aos participantes um cenário de ameaças para ilustrar o procedimento de modelagem da PTMOL. O cenário apresentado como exemplo era diferente do escolhido para o estudo, descartando assim qualquer viés. Após a conclusão do treinamento, o pesquisador (autor da tese) forneceu orientações gerais sobre o protocolo do estudo. Essas orientações incluíam o direito dos participantes de optar por não participar da pesquisa, sem qualquer penalização. Por fim, o pesquisador principal entregou o TCLE e o formulário de caracterização de perfil.

5.3.2 Execução do segundo estudo

O estudo foi executado em um laboratório de informática, o qual disponibilizava computadores para serem utilizados pelos participantes. O pesquisador atuou como instrutor durante a condução do estudo, sendo o principal responsável por auxiliar em casos de dúvidas referente ao processo de aplicação da PTMOL, tomando a devida precaução para não influenciar na atividade de modelagem de ameaças.

Cada participante recebeu os artefatos do estudo, conforme descrito na subseção 5.3.1.3 (instrumentos), realizando as atividades de modelagem individualmente. Todos os artefatos foram disponibilizados por meio do Google Drive[1] Os participantes deveriam

[1]Google Drive é o serviço de armazenamento na nuvem do Google, oferecido tanto em modalidade gratuita como em planos por assinatura (https://www.google.com/drive).

descrever todo o processo de modelagem (e sua lógica) em uma planilha fornecida no estudo. Todos os participantes entregaram ao final do estudo a planilha contendo todas as ameaças identificadas para cada ativo extraído do cenário, os usos maliciosos previstos e as contramedidas associadas, cumprindo todas as tarefas antevistas. As ameaças apareciam na planilha de acordo com sua ordem de descoberta. Além disso, eles também entregaram o modelo de ameaças gerado e a anotação do tempo total gasto na modelagem. Após isso, eles responderam o questionário pós-estudo. Vale ressaltar que, durante a atividade de modelagem, os estudantes não receberam qualquer ajuda do pesquisador envolvido no estudo. O estudo teve duração de aproximadamente quatro horas.

5.3.3 Resultados do segundo estudo

Os documentos devolvidos pelos participantes foram avaliados por três especialistas (o autor da tese e seus orientadores). Os especialistas analisaram as suposições contidas nos *templates* e determinaram se cada uma das ameaças identificadas era aplicável ao cenário em análise. Especificamente, os especialistas determinaram o número de ameaças corretas (verdadeiros positivos) e ameaças incorretas (falsos positivos) com base nas definições fornecidas na subseção 5.3.1.5. Em linhas gerais, ameaças corretas eram aquelas: a) relevantes, relacionadas à privacidade no contexto do cenário fornecido e sólidas em relação às suposições documentadas pelos participantes; b) compatíveis com o catálogo de ameaças da PTMOL; e c) documentadas com bastante detalhe e raciocínio. Além disso, as ameaças que estavam presentes no cenário e que não foram detectadas ou percebidas (falsos negativos) também foram contabilizadas.

5.3.3.1 Oráculo

Um oráculo (solução de referência) foi criado por dois especialistas (Apêndice F). Esse oráculo fornecia uma estimativa aproximada de quantas ameaças de privacidade poderiam ser encontradas no cenário em análise. Os especialistas aplicaram a linguagem PTMOL no cenário, que resultou em 24 ameaças, conforme apresentado na Tabela 5.5. Embora o oráculo seja a referência para a análise quantitativa do estudo, os participantes poderiam fazer suposições que diferem do oráculo. Desse modo, a solução de referência é utilizada apenas como um guia para os avaliadores, que examinaram cuidadosamente o *template* com as suposições feitas por cada participante.

As ameaças de divulgação de informação e clonagem de perfil são as mais recorrentes no cenário de ameaças fornecido. Como havia um número considerável de ativos sendo compartilhados no cenário de ameaças e a possibilidade dos mesmos serem expostos para terceiros, fez com que a ameaça de divulgação de informações fosse a mais recorrente nesse cenário. A ameaça de clonagem de perfil também é frequente no cenário, uma vez que a quantidade de dados pessoais divulgados publicamente pode ser usada para criar um perfil falso da vítima com o propósito de enganar seguidores e capturar informações privadas.

Tabela 5.5: Solução de referência mostrando tipo e número de ameaças por categoria

Ameaças de privacidade	**Número de ameaças**
Clonagem de perfil	6
Divulgação de informação	6
Espionagem	3
Danos à reputação	2
Cyberstalking	2
Reconhecimento facial	2
Inferência/Rastreamento	2
Roubo de identidade	1
Gravação não autorizada	0
Total	**24**

5.3.3.2 Resultados quantitativos do segundo estudo

A Tabela 5.6 consolida os resultados do estudo conduzido. apresentando uma síntese geral da modelagem de ameaças realizada por cada participante do experimento. A primeira coluna (P) representa o código de cada participante (indicados por P01, P02...). A segunda coluna (EP) indica a experiência dos participantes em privacidade. A terceira coluna (EM) indica a experiência dos participantes em modelagem de sistemas. A quarta coluna (PA) representa o número de possíveis ameaças identificadas por participante. A quinta coluna (VP) apresenta o número de verdadeiros positivos, ou seja, o número de ameaças identificadas corretamente. A sexta coluna (FP) indica o número de falsos positivos identificados que não são ameaças. A sétima coluna (FN) revela o número de falsos negativos, ou seja, o número de ameaças não detectadas. A oitava coluna (TG) indica o tempo que cada participante gastou para realizar a atividade de modelagem de ameaças. A nona coluna (Prec.) indica a precisão por participante e a última coluna (Rec.) indica o recall de cada participante.

Inicialmente, com base nos dados fornecidos pela Tabela 5.6, pode-se observar que todos os participantes relataram ter conhecimento em relação a modelagem de sistemas. Por outro lado, todos os participantes relataram não ter experiência em privacidade, eles conheciam apenas alguns conceitos sobre a área adquiridos em leituras/palestras, mas sem nenhuma experiência prática. Ainda que os participantes tenham indicado nenhuma experiência sobre privacidade, eles o dizem com relação à pesquisa sobre privacidade em RSOs, não sobre a importância de cuidar da informação compartilhada e suas possíveis ameaças. Além disso, o fato dos participantes não terem conhecimento prático em privacidade, mas terem experiência em modelagem de sistemas, é um resultado importante sobre o perfil do profissional que vai utilizar a PTMOL. Com isso, esse estudo continua olhando os participantes como designers que estão aprendendo sobre privacidade e tem o potencial de mostrar como esses designers, que não conhecem a linguagem PTMOL, fizeram sentido dela e a utilizaram em um design de ameaças.

Tabela 5.6: Resumo do resultado da modelagem de ameaças por participante

P	EP	EM	PA	VP	FP	FN	TG	Prec.	Rec.
P01	Não	Sim	17	14	3	10	3.45	82.35%	58.33%
P02	Não	Sim	18	17	1	7	3.10	94.44%	70.83%
P03	Não	Sim	19	12	7	12	3.55	63.16%	50.00%
P04	Não	Sim	18	17	1	7	3.17	94.44%	70.83%
P05	Não	Sim	17	16	1	8	3.35	94.12%	66.67%
P06	Não	Sim	18	18	0	6	3.49	100.00%	75.00%
P07	Não	Sim	16	15	1	9	3.25	93.75%	62.50%
P08	Não	Sim	16	16	0	8	2.55	100.00%	66.67%
P09	Não	Sim	20	20	0	4	2.45	100.00%	83.33%
P10	Não	Sim	19	19	0	5	3.32	100.00%	79.17%
P11	Não	Sim	19	18	1	6	3.13	94.74%	75.00%
P12	Não	Sim	21	17	4	7	3.53	80.95%	70.83%

P = Participante, EP = Experiência em privacidade, EM = Experiência em modelagem de sistemas, PA = Possíveis ameaças, VP = Verdadeiro positivo, FP = Falso positivo, FN = Falso negativo, TG = Tempo gasto, Prec. = Precisão, Rec. = *Recall*

No geral, todos os participantes foram capazes de detectar ameaças de privacidade no cenário fornecido com o auxílio da PTMOL. Um baixo número de falsos positivos foi encontrado. Em relação ao número de verdadeiros positivos, nota-se que, em grande parte dos casos, as ameaças apontadas pelos participantes estavam corretas. Esse número superior de verdadeiros positivos pode ser explicado por dois fatores: a) treinamento prévio, que possibilitou o esclarecimento de dúvidas específicas quanto ao processo de aplicação da PTMOL e permitiu também uma discussão abrangente sobre os elementos da linguagem; e b) experiência dos participantes, que estavam cursando uma disciplina de Segurança de Sistemas em um período mais avançado, além da experiência em modelagem de sistemas. Portanto, pode-se observar que o fator de treinamento e conhecimento sobre PTMOL pode ser mais importante do que o fator de experiência em privacidade. Isso fica claro ao examinar os dados fornecidos na Tabela 5.6, pois todos os participantes conseguiram mapear cenários de ameaças, mesmo que não fossem especialistas em segurança e privacidade. Isso indica que a PTMOL pode auxiliar os projetistas de software na modelagem de ameaças sem exigir um alto nível de especialização na área de privacidade.

A maioria das possíveis ameaças listadas pelos participantes eram verdadeiros positivos, ou seja, foram identificadas corretamente. Os participantes P06, P08, P09 e P10 detectaram o maior número de ameaças no cenário e todas estavam corretas, o que indica 100% de precisão em seus diagnósticos de ameaças. No entanto, o participante P03 obteve a menor precisão (63,16%) e também o maior número de falsos positivos na modelagem de ameaças. Além disso, embora a PTMOL tenha possibilitado a identificação das ameaças corretas, nem todas as ameaças presentes no cenário foram percebidas ou detectadas. Isso justifica o número de falsos negativos e a taxa relativamente baixa do *recall* por participante.

Para analisar de forma mais específica os resultados quantitativos, análises estatísticas foram efetuadas usando o teste de normalidade de Shapiro-Wilk. O teste de normalidade testa a hipótese de que os dados apresentam uma distribuição normal. No caso de amostras menores (<30 casos), o teste Shapiro-Wilk é o mais indicado (Lazar and Barbosa, 2017). Nesses testes, se a significância do teste de normalidade for menor que 0,05, então a distribuição da amostra não é normal. Se for maior que 0,05, pode-se dizer que a distribuição da amostra é normal (Lazar and Barbosa, 2017). O teste de normalidade mostrou que os dados do estudo de viabilidade não têm distribuição normal (com p=0,001).

De acordo com Lazar and Barbosa (2017), quando uma amostra não segue uma distribuição normal, deve-se usar um teste não paramétrico. A partir disso, o teste de Wilcoxon foi selecionado. Em linhas gerais, o teste de Wilcoxon é um teste de hipóteses para comparar a diferença entre duas medidas de uma mesma amostra, ou seja, quando os resultados dos participantes são medidos sob duas condições diferentes (Rey and Neuhäuser, 2011). Para realizar a comparação, os dados são ranqueados de acordo com a diferença entre as duas medidas pareadas. Ao final, o teste de Wilcoxon dará um resultado de hipóteses, onde deve-se rejeitar a hipótese nula quando $p < 0,05$ e aceitar que há diferença entre as medidas comparadas. Para representar um resumo dos resultados destas análises foi utilizado o gráfico de *boxplot*. As análises foram executadas por meio do uso da ferramenta estatística SPSS, considerando um alpha (nível de significância) menor que 0,05 para refutar a hipótese nula.

Corretude. O primeiro conjunto de hipóteses refere-se a corretude, conforme descrito na subseção 5.3.1.5. Nesse sentido, o teste de Wilcoxon foi aplicado para comparar se havia diferença estatística entre o número de verdadeiros positivos em relação ao número de falsos positivos diagnosticados no estudo. Como hipótese para o teste estatístico, tinha-se a não diferença entre as médias das medidas relacionadas.

A Figura 5.8 demonstra os *boxplots* comparando o número de: (i) verdadeiros positivos (ameaças identificadas corretamente); (ii) falsos negativos (ameaças não detectadas ou percebidas no cenário); e (iii) falsos positivos (ameaças incorretas). Com base na representação gráfica ilustrada pela Figura 5.8, pode-se observar que o número de falsos positivos é bastante inferior comparativamente ao de verdadeiros positivos. A média para o número de verdadeiros positivos foi de 16,58 (com um desvio padrão de 2,193) e o intervalo de confiança de 95% (teste de Wilcoxon de uma amostra). Em média, apenas 1,58 falsos negativos (desvio padrão é 2,109) foram encontrados, com um intervalo de confiança de 95%. Em vista disso, o teste de Wilcoxon confirmou que o número de verdadeiros positivos foi significativamente superior ao número de falsos positivos ($p = 0,002$). Portanto, há evidências para rejeitar a hipótese nula H01. Em síntese, esses resultados sugerem que a PTMOL consegue diagnosticar um número maior de ameaças corretas do que de ameaças incorretas, evidenciando um nível adequado de precisão e corretude.

Completude. O segundo conjunto de hipóteses diz respeito a completude, conforme descrito na subseção 5.3.1.5. No contexto da completude, o teste de Wilcoxon foi aplicado para comparar se havia diferença estatística entre o número de verdadeiros

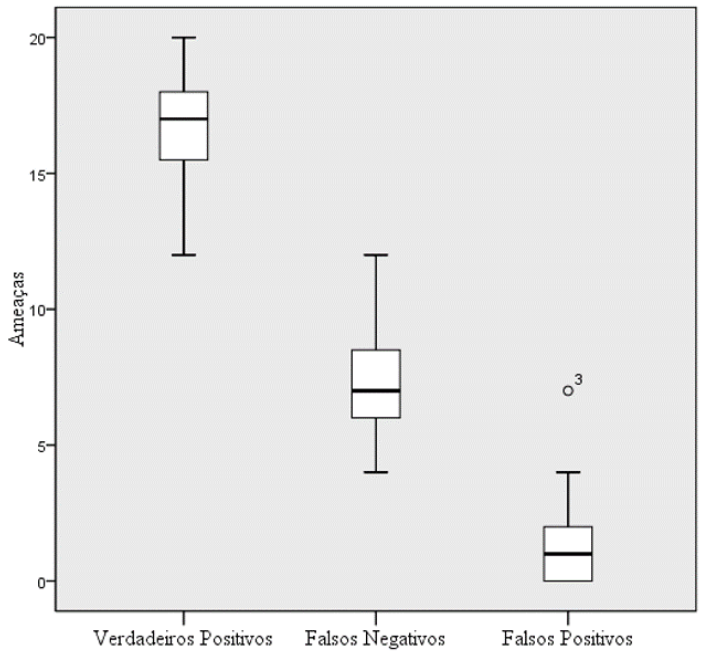


Figura 5.8: *Boxplot* comparando os verdadeiros positivos, falsos negativos e falsos positivos

positivos em relação ao número de falsos negativos. A partir dessa disso, formulou-se como hipótese para o teste estatístico a não diferença entre as médias dessas medidas relacionados.

Conforme ilustrado anteriormente na Figura 5.8, é possível observar que o número de falsos negativos (ameaças não detectadas ou não percebidas no cenário) é inferior ao número total de verdadeiros positivos. Ao relacionar as duas medidas usando o teste não paramétrico de Wilcoxon, também foi identificada diferença estatística ($p = 0{,}003$). Portanto, os resultados do teste estatístico apoiam a hipótese alternativa HA2 – "*O número de ameaças identificadas corretamente (verdadeiros positivos) é maior que o número de ameaças não detectadas ou percebidas no cenário de ameaças (falsos negativos)*" e, portanto, pode-se refutar a hipótese nula H02.

A Figura 5.9 traz uma representação gráfica indicando a média de verdadeiros positivos (barras brancas), falsos negativos (barras cinzas) e falsos positivos (barras pretas) para cada ameaça presente no cenário. Assim como no oráculo, a "Divulgação de informações" e a "Clonagem de perfis" foram as ameaças mais apontadas pelos participantes durante o processo de modelagem. "Cyberstalking" e "Roubo de identidade" foram as que obtiveram o maior número de falsos positivos. Isso pode ser explicado pelo fato de que as ameaças supracitadas possuem semânticas relativamente semelhantes, o que pode ter causado algum equívoco entre os conceitos. Tal questão pode ser um indício de que a descrição geral dessas ameaças deve ser revisada para evitar redundâncias.

Por fim, a ameaça de "Gravação não autorizada" não se aplica ao cenário mapeado.

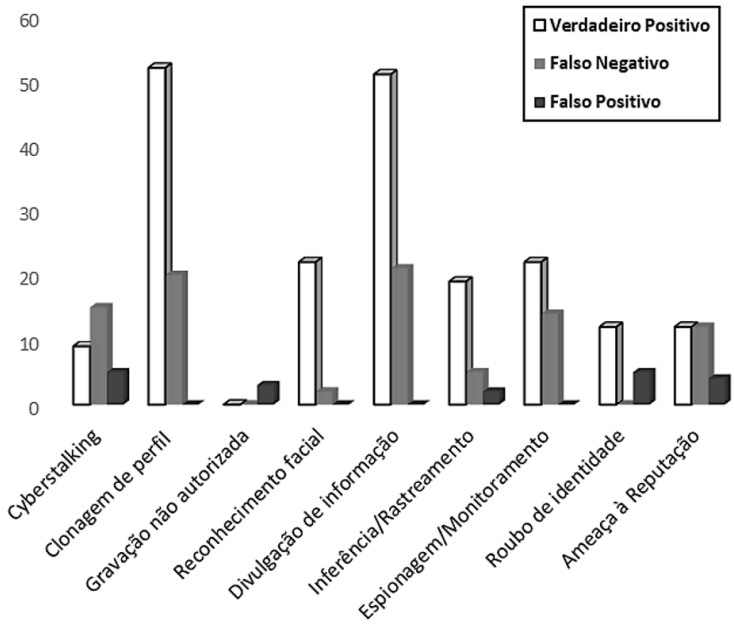


Figura 5.9: Média do número de verdadeiros positivos, falsos negativos e falsos positivos para cada ameaça do catálogo PTMOL

No geral, todos os participantes foram capazes de identificar e examinar a maior parte das ameaças existentes no cenário fornecido no estudo. Isso indica que a PTMOL foi capaz de propiciar um mapeamento considerável de ameaças corretas, indicando com isso sua viabilidade prática como uma linguagem para a modelagem de ameaças de privacidade.

Produtividade. Além do conjunto de hipóteses formuladas para completude e corretude, formulou-se também uma hipótese para a produtividade, conforme detalhado na subseção 5.3.1.5. A Figura 5.10 apresenta os *boxplots* que resumem a quantidade de esforço dedicado (tempo gasto) pelos participantes a cada etapa do processo de modelagem PTMOL. A etapa de identificação de ativos teve um tempo total de duração de 4,33 horas (*boxplot* ativos). A etapa de identificação de ameaças e usos maliciosos previstos durou cerca de 17,39 horas (*boxplot* de ameaças). A etapa de seleção de contramedidas teve um tempo total de 7,2 horas gastas (*boxplot* de contramedidas). Por fim, a etapa de geração do modelo de ameaça levou cerca de 8,91 horas (*boxplot* modelo). Portanto, os participantes gastaram um total de 37 horas para aplicar as etapas do processo de modelagem com a PTMOL, sendo que a maior parte foi dedicada à etapa de identificação de ameaças, conforme esperado.

Para calcular a produtividade, a quantidade de esforço foi utilizada como parâmetro de comparação em relação ao esforço real realizado durante o processo de modelagem. Como a produtividade está estritamente interessada apenas em resultados

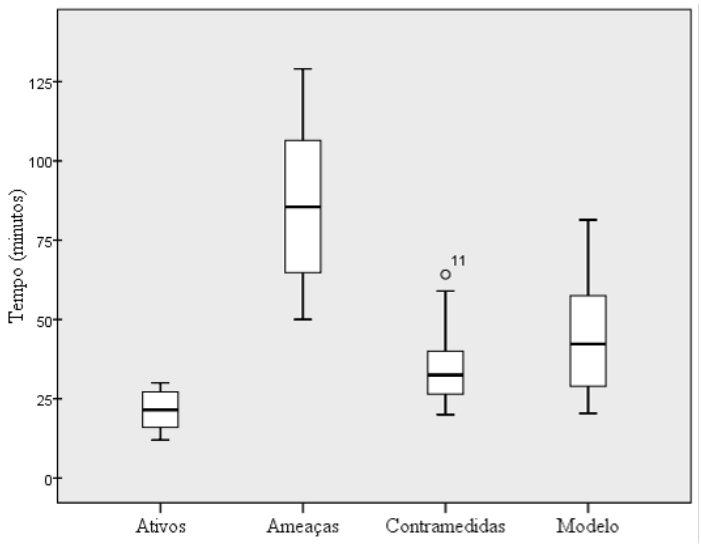


Figura 5.10: *Boxplots* para a quantidade de esforço dedicado (tempo gasto) pelos participantes para cada etapa do processo de modelagem PTMOL

corretos, considerou-se apenas o número de ameaças corretamente identificadas (verdadeiros positivos) pelo tempo total gasto (esforço real), conforme formulado na hipótese. Em média, a produtividade dos participantes foi de 5,26 ameaças por hora. Isso indica que a produtividade está muito acima do esperado e a hipótese nula H03 foi refutada.

5.3.3.3 Análise da percepção dos participantes sobre a PTMOL

Os participantes indicaram seu grau de aceitação sobre a PTMOL por meio de um questionário pós-estudo. Esse questionário foi elaborado com base nos indicadores do modelo TAM (*Technology Acceptance Model*) Davis (1989). A partir da fundamentação teórica fornecida pelo TAM, três indicadores principais foram escolhidos:

- **Facilidade de uso percebida**: Define o grau em que o participante acredita que usar a PTMOL para modelar ameaças de privacidade seria livre de esforço.
- **Utilidade percebida**: Define o grau em que o participante acredita que a PTMOL poderia melhorar seu desempenho na modelagem de ameaças de privacidade em RSOs.
- **Satisfação percebida**: Define o grau em que o uso da PTMOL para modelar ameaças de privacidade em RSOs é percebido como prazeroso, além de quaisquer consequências de desempenho do uso.

É importante destacar que foram utilizados os mesmos indicadores do primeiro estudo, com exceção do "intenção de uso futuro". Como os resultados do primeiro estudo para esse indicador foram positivos, utilizou-se outro indicador, satisfação percebida, de

modo a testar a experiência de uso percebida sobre a aplicabilidade da PTMOL. Para cada indicador do segundo estudo, foi estabelecido um conjunto de variáveis com uma escala composta por seis pontos. A escala utilizada é de natureza ordinal, variando de 6 (concordo totalmente) a 1 (discordo totalmente). O grau de concordância cresce de acordo com o maior número de pontos. Conforme sugerido por Laitenberger and Dreyer (1998), o ponto neutro (nem concorda nem discorda) não foi utilizado na escala ordinal, pois não permite identificar a inclinação (positiva ou negativa) dos participantes. Além disso, não utilizar o ponto neutro ajuda a evitar o viés de tendência central nas avaliações, obrigando os participantes a julgar o resultado como adequado ou inadequado.

Facilidade de uso percebida. A tabela 5.7 apresenta os resultados da percepção dos participantes quanto à facilidade de uso da PTMOL para modelagem de ameaças de privacidade. No geral, os dados apresentados na Tabela 5.7 indicam resultados positivos para todas as variáveis do indicador em questão. No entanto, também houve discordâncias envolvendo algumas variáveis. Algumas falas dos participantes indicam fatores que podem ter influenciado esse resultado:

"Embora existam apenas alguns elementos na notação, mas senti falta de alguns, por exemplo, onde entraria quem pode cometer os usos maliciosos?" - P12.

"É fácil aprender a linguagem, mas o processo de modelagem é difícil. Requer tempo e muita atenção" - P07.

"Achei fácil de usar, embora exija certo nível de atenção aos detalhes na modelagem do cenário" – P03.

"A linguagem é simples, porém usar pela primeira vez parece um pouco complicado pela quantidade de informações, mas não seria difícil tornar isso um hábito" - P01.

Tabela 5.7: Percepção dos participantes sobre a facilidade de uso da PTMOL

Nº	**Variáveis**	**GC(%)**	**GD(%)**
F1	A PTMOL é fácil de aprender	91,67%	8,33%
F2	Foi fácil utilizar a PTMOL para modelar ameaças de privacidade	83,33%	16,67%
F3	Os elementos da PTMOL são claros e fáceis de entender	75,00%	25,00%
F4	A PTMOL é fácil de usar	91,67%	8,33%

GC = Grau de concordância, GD = Grau de discordância.

As citações feitas pelos participantes indicam que, no geral, a linguagem PTMOL é fácil de aprender e usar. No entanto, a linguagem requer um esforço inerente para executar seu processo metodológico. Por se tratar de modelagem conceitual destinada para ser aplicada em nível de design, os resultados produzidos pela equipe de design precisam ser detalhados o suficiente para garantir uma interpretação de qualidade do cenário de ameaça ao qual um usuário pode estar exposto. Portanto, pode-se observar que a PTMOL possui um grau relevante de facilidade de uso, mas demanda um esforço peculiar em termos de duração e dedicação ao processo de modelagem.

Utilidade percebida. A tabela 5.8 exibe os resultados relacionados à percepção sobre a utilidade da PTMOL para modelagem de ameaças de privacidade. O indicador de utilidade geralmente demonstra uma probabilidade subjetiva percebida pelo usuário de que a solução proposta pode melhorar o desempenho em relação ao objeto de uso. Nesse sentido, analisando a percepção dos participantes quanto à utilidade da PTMOL, é possível notar resultados positivos para as variáveis U2, U3 e U4. Algumas citações justificam tais resultados:

- "É bastante interessante modelar ameaças com a PTMOL" - P01.

- "Achei muito útil modelar as ameaças com a linguagem porque tem um procedimento simples, mas que é bem detalhado, e autoexplicativo" - P10.

- "Uma abordagem muito importante e definitivamente me fez pensar sobre privacidade de uma forma que eu não tinha pensado antes" - P11.

- "Permite fazer uma avaliação bem feita e válida, além de levantar situações que abordam questões importantes de privacidade" - P05.

Tabela 5.8: Percepção dos participantes sobre a utilidade da PTMOL

Nº	Variáveis	GC(%)	GD(%)
U1	Usando uma linguagem como a PTMOL, eu seria capaz de modelar ameaças de privacidade em RSOs mais rapidamente	91,67%	8,33%
U2	Usar a PTMOL melhoraria meu desempenho na modelagem de ameaças de privacidade em RSOs (acredito que eu iria identificar um número de ameaças maior, em um tempo menor, do que levaria sem usar esta linguagem)	100,00%	0,00%
U3	Usar a PTMOL para modelar ameaças de privacidade em RSOs aumentaria minha produtividade	100,00%	0,00%
U4	Considero a PTMOL útil para modelar ameaças de privacidade em RSOs	100,00%	0,00%

GC = Grau de concordância, GD = Grau de discordância.

Satisfação percebida. Em relação à satisfação percebida sobre a PTMOL para modelagem de ameaças, foram obtidos resultados positivos para todas as afirmações de acordo com as opiniões dos participantes. Não houve divergências, conforme mostra a Tabela 5.9, em relação às variáveis do indicador em questão, sugerindo que a PTMOL, embora tenha um esforço inerente em relação ao seu contexto de uso, fornece um boa experiência ao designer durante sua aplicação. No entanto, alguns participantes apontaram o perfil do profissional que utilizará a PTMOL como um fator que pode influenciar na experiência de uso.

"Acredito que a pessoa tem que ter prática e experiência em privacidade e segurança, se a pessoa não tiver isso pode impactar na aplicação e tornar o processo de modelagem tedioso" -P03.

"A PTMOL é bom para quem já tem conhecimento" - P02.

As citações feitas pelos participantes destacam um fator que deve ser observado em relação ao processo de modelagem da PTMOL, que é a necessidade de conhecimento prévio em privacidade de sistemas. No geral, a PTMOL foi proposta para ser aplicada

Tabela 5.9: Satisfação percebida dos participantes sobre a PTMOL

Nº	Variáveis	GC(%)	GD(%)
S1	Usar a PTMOL pode ser agradável	100,00%	0,00%
S2	O processo atual de modelagem de ameaças da PTMOL é prazeroso	100,00%	0,00%
S3	Eu me divirto usando a PTMOL	100,00%	0,00%

GC = Grau de concordância, GD = Grau de discordância.

por designers de software sem necessariamente exigir conhecimento técnico deles. Todos os participantes do estudo eram alunos com certo grau de conhecimento acadêmico em modelagem de software e segurança de sistemas, mas que não possuíam conhecimento técnico sobre o tema de fundo. Portanto, entende-se que alunos são profissionais menos experientes e, portanto, foram classificados como designers novatos.

Nessa perspectiva, os resultados indicam que o fator conhecimento técnico não pode considerado necessário para aplicação da PTMOL, pois todos os participantes, que não eram especialistas, conseguiram executar todo o processo de aplicação da linguagem e produziram resultados satisfatórios. Os recursos e procedimentos autoexplicativos da PTMOL servem como um guia para auxiliar na modelagem e garantir um design efetivo de ameaças de privacidade. Portanto, pode-se concluir que o fator conhecimento prévio em segurança e privacidade não deve ser visto como pré-requisito para a execução da PTMOL.

5.3.4 PTMOL comparada a outras metodologias de modelagem de ameaças

Nos trabalhos de Wuyts et al. (2014) e Scandariato et al. (2015), os autores também avaliaram a completude, a corretude e a produtividade das suas soluções para modelagem de ameaças. O design experimental deste estudo é baseado no mesmo protocolo aplicado para avaliar o LINDDUN e o STRIDE. Portanto, pode ser útil comparar os resultados obtidos em cada estudo. Vale ressaltar que, embora a configuração seja comparável, os estudos foram executados de forma independente, portanto, nenhuma conclusão estatística deve ser considerada. A Tabela 5.10 resume os resultados obtidos em cada estudo em relação as métricas avaliadas.

Tabela 5.10: PTMOL comparada a outras metodologias para modelagem de ameaças

Métricas	PTMOL	LINDDUN	STRIDE
Precisão	91%	71%	81%
Recall	69%	56%	36%
Produtividade	5 ameaças/hora	0,5 ameaça/hora	1 ameaça/hora

Corretude. A precisão dos resultados no estudo realizado com o método STRIDE foi de 81% e com o LINDDUN foi equivalente a 71%. A precisão da PTMOL no estudo de viabilidade foi superior, com o resultado de 91%, comparativamente

aos métodos referidos. Embora sejam soluções com procedimentos metodológicos diferentes, todas possuem o foco em modelagem de ameaças. Portanto, os resultados da precisão são comparáveis.

Completude. Em relação à completude, os resultados da PTMOL mostram uma taxa para o *recall* de 69%. LINDDUN obteve uma taxa baixa para o *recall*, 56% e método STRIDE executou a menor taxa de todas, com apenas 36%. Ainda que a PTMOL tenha obtido um resultado abaixo do esperado para o indicador em questão, sua taxa é superior quando comparada a das outras metodologias.

Produtividade. A produtividade da PTMOL foi de 5 ameaças por hora, indicando um resultado muito acima do esperado. O método STRIDE resultou em 1 ameaça por hora, o que configura uma produtividade baixa. Por fim, o método LINDDUN obteve um desempenho bastante inferior em termos de produtividade, com apenas meia (0,5) ameaça por hora. Novamente, a PTMOL apresenta uma produtividade superior quando comparada a outros métodos.

5.3.5 Melhorias na PTMOL após a execução do segundo estudo

No geral, os resultados do segundo estudo apontaram necessidades de melhorias quanto ao indicador de completude da PTMOL. Com isso, após as análises realizadas às questões abertas contidas no questionário pós-estudo, observou-se que poucos ajustes na estrutura da PTMOL seriam pertinentes, uma vez que nenhum participante reportou alguma dificuldade relevante quanto ao procedimento metodológico da linguagem.

Para ajustar ou acrescentar algum elemento na linguagem, buscou-se analisar os principais questionamentos e feedbacks fornecidos pelos participantes do estudo, de modo a identificar alguma melhoria relevante. Um ponto citado por um dos participantes sobre quem seriam os agentes da ameaça, provocou uma reflexão significativa sobre um elemento não previsto na linguagem PTMOL. De fato, podem existir diversas fontes maliciosas dentro ou fora da RSO que têm o propósito de violar a privacidade do usuário. Indicar a fonte responsável pela ameaça traz uma complementação ao processo de modelagem da PTMOL e ajuda a refletir de forma mais correta sobre os usos maliciosos que aquela determinada fonte poderá produzir. Com isso, criou-se o elemento "fontes de vazamento", o qual foi classificado em 4 tipos:

- Um **membro malicioso** infiltrado na própria RSO do usuário, que pode ser um amigo ou um seguidor;
- Um **provedor de serviços** da rede, que pode fazer uso indevido dos dados privados do usuário;
- Um **aplicativo terceirizado**, que tem acesso ou faz uso indevido dos dados do usuário;
- **Fontes externas**, que não estão diretamente infiltradas nas RSOs, mas conseguem coletar e obter dados do usuário vinculados em outros sites, como mecanismos de busca, por exemplo.

5.3.6 Limitações do segundo estudo

Todo estudo possui limitações em seus resultados e elas precisam ser relatadas. Dentre as limitações deste estudo, destacamos três principais. A primeira está relacionada com o fato dos participantes serem estudantes de graduação e o estudo ser conduzido em um ambiente acadêmico. Sobre isto, Fernandez et al. (2012) afirmam que estudantes que não têm experiência na indústria podem, no entanto, ter habilidades semelhantes aos profissionais menos experientes. Portanto, apesar da limitação imposta pela participação de estudantes no estudo e não de profissionais, acredita-se que os resultados encontrados não devem ser considerados inválidos.

Outra limitação pode estar relacionada a generalização dos resultados obtidos. A quantidade de participantes envolvidos no estudo não pode ser considerada como representativa, porém buscou-se mitigar essa ameaça pela obtenção e coleta de dados relevantes sobre o processo de aplicação da PTMOL. Todavia, nem todos os resultados obtidos puderam ser utilizados para contribuir para uma conclusão estatística mais efetiva.

Por fim, outra limitação trata-se da possibilidade do autor principal da pesquisa ter introduzido seu viés no processo de análise de dados. A este respeito, o processo de análise foi supervisionado por outro dois pesquisadores mais experientes. Esses pesquisadores revisaram e analisaram todos os resultados intermediários, tais como os dados quantitativos e qualitativos. Esse processo iterativo foi repetido até o final da coleta e análise de dados.

5.3.7 Conclusões do segundo estudo

A análise quantitativa do segundo estudo experimental indicou bons resultados para a corretude (taxa acima de 80%) e completude (taxa acima de 60%) do processo de modelagem de ameaças da PTMOL. Os resultados para os indicadores de utilidade, facilidade de uso e satisfação percebida da linguagem foram, no geral, positivos, embora alguns participantes discordassem do aspecto facilidade de uso. Por se tratar de uma modelagem conceitual destinada para ser aplicada em nível de design, os resultados produzidos pela equipe de design precisam ser detalhados o suficiente para garantir uma interpretação de qualidade do cenário de ameaça sob análise. Portanto, embora a PTMOL apresente um grau relevante de facilidade de uso, sua aplicação pode demandar um esforço inerente em termos de duração e dedicação ao processo de modelagem.

Além disso, os resultados do segundo estudo também apontaram indícios de que a PTMOL é aplicável até mesmo por profissionais não especialistas em privacidade, pois todos os participantes conseguiram mapear cenários de ameaças mesmo não tendo conhecimento técnico. Isso pode ser um indicador de que a PTMOL pode ser incorporada ao desenvolvimento de RSOs durante a fase de design e pode auxiliar designers de software na modelagem de ameaças, sem exigir um alto nível de especialidade na área de privacidade.

Por fim, por meio de comentários e feedbacks fornecidos pelos participantes do estudo, também foram identificadas oportunidades de melhorias a serem implementadas

na PTMOL, como a necessidade de incluir e adaptar elementos da linguagem para permitir uma modelagem de ameaças mais efetiva e completa. Todas as melhorias foram implementadas e uma terceira versão da PTMOL foi criada. Com uma nova versão da linguagem, decidiu-se conduzir um estudo de observação para investigar de forma mais aprofundada o uso da PTMOL no processo de modelagem de ameaças em RSOs. Esse estudo traz um enfoque mais qualitativo para buscar outras melhorias que podem ser necessárias para a linguagem. A próxima seção descreve o planejamento, execução e resultados do terceiro estudo aplicado com a PTMOL.

5.4 Terceiro Estudo: Estudo de Observação

Uma vez que os resultados obtidos com os estudos anteriores indicaram a validade e viabilidade da PTMOL, prosseguiu-se então para um próximo estudo com o propósito de responder a seguinte questão de pesquisa: "*Os passos do processo fazem sentido*?". Para responder essa questão, realizou-se um estudo de observação (Shull et al., 2001) visando compreender de forma mais aprofundada o processo utilizado pelos designers ao aplicar a PTMOL durante uma modelagem de ameaças de privacidade, bem como identificar as situações nas quais as dificuldades no uso da PTMOL podem ocorrer. Segundo Shull et al. (2001), em um estudo de observação, os dados podem ser coletados ou obtidos de forma observacional ou inquisitiva. Dados observacionais podem ser coletados durante o uso de uma solução sem a interferência do pesquisador. Em contrapartida, dados inquisitivos são geralmente coletados após o fim de uma avaliação, onde o pesquisador indaga os participantes sobre os aspectos de uso relacionados à solução.

Para o contexto deste estudo, aplicou-se tanto técnicas de cunho observacionais como inquisitivas. Para a coleta de dados observacionais, utilizou-se como base a técnica de *design rationale* (Lee, 1997) para registrar as decisões de melhorias para a PTMOL. Para a coleta de dados inquisitivos, utilizou-se a técnica de grupo focal (Pelicioni et al., 2001).

5.4.1 Planejamento

Os participantes do estudo foram dezenove (19) estudantes de graduação dos cursos de Ciência da Computação e Engenharia de Software, da UFAM. Os alunos cursavam a disciplina de Segurança de Sistemas Computacionais e foram escolhidos por critérios de conveniência. Essa escolha deu-se principalmente por acessibilidade que, segundo Vergara (2003), longe de qualquer procedimento estatístico, esse critério seleciona elementos pela facilidade de acesso a eles. A escolha também deu-se em razão dos alunos terem um potencial conhecimento/consciência sobre ameaças, uma vez que estes estavam cursando uma disciplina de Segurança de Sistemas. Ressalta-se que nenhum dos participantes desse estudo tinham participado dos estudos anteriores.

Os participantes tiveram acesso a um termo de consentimento livre e esclarecido (Apêndice 6.4), que informava o motivo da pesquisa e como seriam utilizados os dados

obtidos, de maneira que eles pudessem tomar a sua decisão de forma justa e sem constrangimentos sobre a sua participação. Somente após o aceite desses termos a pesquisa foi iniciada. Os participantes deveriam formar equipes compostas por 4 a 6 integrantes. Diferente dos estudos anteriores, onde cada participante realizava sua modelagem de ameaças de forma individual, para o contexto deste estudo, os participantes deveriam efetuar as atividades de modelagem em grupo. O total de grupos formados pelos participantes foram 04. A Tabela 5.11 apresenta a caracterização dos participantes do terceiro estudo com a PTMOL.

Tabela 5.11: Caracterização dos participantes do terceiro estudo com a PTMOL

Participantes	**Grupo 01**	**Grupo 02**	**Grupo 03**	**Grupo 04**
Sexo feminino	2	0	2	2
Sexo masculino	2	4	3	3
Total	**4**	**4**	**6**	**5**

5.4.2 Execução do terceiro estudo

O estudo foi planejado para ser executado em três dias. No primeiro dia, os participantes receberam um treinamento geral sobre o processo de aplicação da PTMOL e testaram as etapas da modelagem de ameaças para o cenário fornecido (Apêndice C). Esse treinamento durou aproximadamente duas horas. O cenário utilizado como exemplo durante o treinamento foi diferente do escolhido para o estudo, descartando assim qualquer possibilidade viés. Ressalta-se ainda que essa primeira etapa também funcionou como um pré-teste, permitindo que todas as eventuais dúvidas sobre o processo de modelagem pudessem ser sanadas. Após a conclusão do treinamento, o autor da tese forneceu as principais informações sobre o protocolo do estudo. Essas orientações incluíam o direito dos participantes de optar por não participar da pesquisa, sem qualquer penalização.

No segundo dia do estudo, os participantes, reunidos em grupos, realizaram a modelagem de ameaças para o cenário fornecido, onde cada equipe aplicou as seguintes tarefas: (i) identificar ativos; (ii) identificar ameaças de privacidade; (iii) prever os usos maliciosos; e (iv) identificar contramedidas. Ao final do segundo dia do estudo, as equipes entregaram os *templates* de modelagem contendo todas as ameaças identificadas no cenário, os usos maliciosos previstos e as contramedidas associadas. Essa etapa durou aproximadamente duas horas. Por fim, no terceiro e último dia do estudo, realizou-se a coleta de dados sobre a experiência de uso da PTMOL, a qual será detalhada na próxima subseção.

5.4.3 Coleta de dados

Após a conclusão da segunda etapa do estudo, os alunos participaram de uma coleta de dados para relatarem suas experiências e percepções ao executarem as atividades de modelagem da PTMOL. Nessa etapa, buscou-se obter dados significativos

sobre as facilidades e/ou dificuldades em compreender o que é modelar ameaças de privacidade no contexto de RSOs, bem como obter oportunidades para o refinamento da linguagem. Para obter essas reflexões qualitativas e ganhar novos *insights* quanto ao processo de aplicação da PTMOL, utilizou-se duas técnicas para a coleta de dados, grupo focal e *design rationale*. A seguir, será descrito como cada técnica foi aplicada.

5.4.3.1 Grupo focal

A primeira parte da coleta de dados com os participantes foi realizada por meio de grupo focal, técnica que permite obter dados a partir de reuniões em grupos e possibilita o entendimento do ponto de vista da população em análise. Pode ser utilizada no entendimento das diferentes percepções e atitudes acerca de uma solução (Pelicioni et al., 2001). O roteiro utilizado para aplicar essa técnica baseou-se nos trabalhos de de França et al. (2015) e Marques et al. (2017).

Durante a sessão do grupo focal, os participantes deveriam discutir sobre os principais aspectos positivos e negativos relacionados à utilidade, facilidade de uso e facilidade de aprendizado da PTMOL. Para fomentar as discussões e provocar as equipes a exporem suas diferentes percepções, utilizou-se no grupo focal a dinâmica de *lovers x haters* (de França et al., 2015; Marques et al., 2017). Durante essa dinâmica, os participantes definidos com o papel de *lovers* deveriam apresentar argumentos a favor da linguagem PTMOL, enquanto que os *haters* deveriam contrapor a equipe com argumentos críticos a linguagem.

A partir disso, criou-se duas equipes para aplicar o grupo focal e cada participante foi alocado em uma determinada equipe. A escolha dos papéis de cada integrante das equipes (*lover* ou *hater*) foi definida por meio de sorteio. Houve um maior número de integrantes para a equipe *haters*, uma vez que o objetivo do grupo focal era obter *insights* relevantes sobre o processo de aplicação da PTMOL e coletar oportunidades de incrementos. Para conduzir a discussão com a dinâmica *lovers x haters*, foi elaborado um quadro com três tópicos a serem debatidos, cada um referente à utilidade, facilidade de uso e facilidade de aprendizado da PTMOL (Figura 5.11). As equipes tiveram 10 minutos para discutir internamente dois argumentos sobre cada tópico em questão. Após essa discussão interna sobre os tópicos mostrados na Figura 5.11, eles deveriam registrar cada argumento em *post-its* e anexá-los no quadro de acordo com o tópico específico. Após isso, a sessão de grupo focal foi iniciada e discutida na seguinte ordem: (i) utilidade da PTMOL; (ii) facilidade de uso da PTMOL e facilidade de aprendizado da PTMOL. As equipes foram encorajadas a lerem seus argumentos e discuti-los uns contra os outros. Após o primeiro argumento, uma equipe contrária dava continuidade à discussão rebatendo o argumento anterior. Este fluxo foi seguido até que todas as equipes tivessem apresentado seus argumentos.

Dois pesquisadores estiveram envolvidos na condução do grupo focal. Um mediador conduziu as discussões para mantê-las em foco, estimulando os participantes a exporem seus argumentos a favor ou contra os tópicos supracitados e discutirem suas opiniões, de acordo com seus papéis definidos. Paralelamente, o outro pesquisador anotava as observações em relação à dinâmica utilizada. Todo o áudio da sessão do

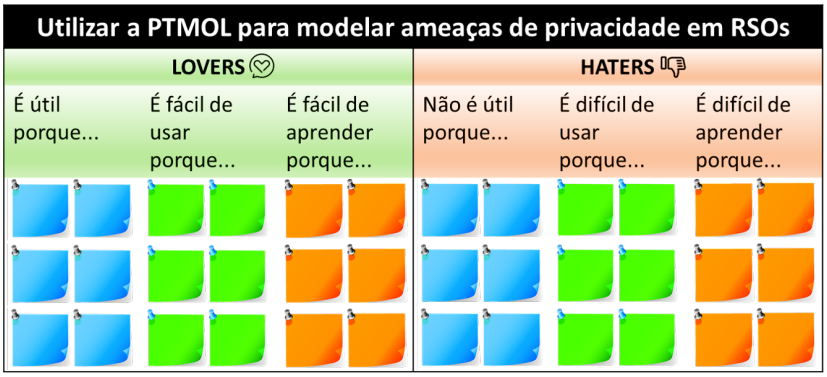


Figura 5.11: Quadro com os tópicos de discussão do grupo focal
Fonte: Adaptado de Marques et al. (2017).

grupo focal foi gravado para posterior análise. Também foi utilizado para a análise dos dados os argumentos fornecidos nos *post-its* e as anotações feitas pelo pesquisador durante o estudo de observação.

5.4.3.2 Design *Rationale*

Para coletar sugestões de melhorias e oportunidades de refinamento sobre o uso da PTMOL, após a finalização da sessão de coleta de dados por meio do grupo focal, os participantes se reuniram novamente com as suas equipes para registrar as decisões e sugestões de aprimoramento por meio de um template baseado em design *rationale* (DR). Em linhas gerais, a técnica de DR pode ser aplicada com o propósito de registrar as razões e justificativas em torno de uma decisão, as alternativas consideradas ou descartadas, ou os argumentos que conduziram à decisão final de um design. Essas decisões a serem registradas poderiam estar relacionadas principalmente à dúvidas quanto as fases de aplicação do processo de modelagem da PTMOL, dúvidas sobre algum elemento e associação entre eles, ou dúvidas gerais sobre qualquer recurso de aplicação da PTMOL. A Figura 5.12 ilustra um exemplo de registro de decisão de design fornecido para as equipes.

5.4.4 Procedimento de análise dos dados

Os dados coletados durante o estudo de observação foram transcritos e posteriormente importados e analisados com apoio do software Atlas.ti[2]. Os dados foram analisados utilizando os procedimentos da Teoria Fundamentada nos Dados (*Grounded Theory – GT*). O *Grounded Theory* é um método de pesquisa qualitativo que utiliza um conjunto de procedimentos sistemáticos de coleta e análise dos dados para gerar, elaborar e validar teorias substantivas sobre fenômenos essencialmente sociais (Glaser et al., 1968). GT baseia-se na ideia de codificação *(coding)*, que é o processo de analisar

[2]https://atlasti.com/

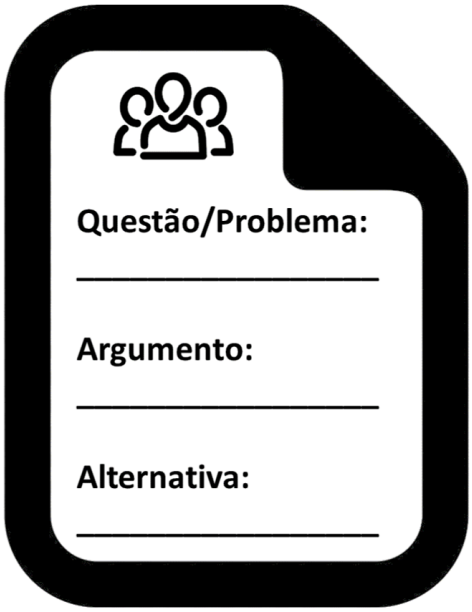


Figura 5.12: Documento para registro de decisão de *design rationale* fornecido para as equipes

Fonte: Próprio autor.

os dados. Durante a codificação são identificados conceitos (ou códigos) e categorias. Um código indica um fenômeno de interesse que tem um significado para o pesquisador (Corbin and Strauss, 2014). Categorias são agrupamentos de códigos unidos em um grau de abstração mais elevado. Dos procedimentos do GT, foram utilizadas a codificação aberta, a codificação axial, mas não a codificação seletiva. A codificação aberta envolve a repartição, análise, comparação, conceituação, e a categorização dos dados. A codificação axial examina as relações entre as categorias identificadas. A codificação seletiva realiza o refinamento de todo esse processo, identificando uma categoria central com o qual todos as outras categorias são relacionadas.

Inicialmente, realizou-se a codificação aberta (primeira fase) associando códigos com citações de transcrições. Em seguida, os códigos foram agrupados de acordo com suas propriedades, formando conceitos que representam categorias mais abstratas. Os procedimentos da codificação aberta estimulam a constante criação de novos códigos e a fusão com os códigos existentes quando novos dados de evidência e interpretação emergem. Por fim, os códigos foram relacionados entre si – codificação axial (segunda fase). Uma vez preparados, os códigos e as redes identificadas nas categorias foram revistos e analisados por outros pesquisadores. Os códigos e categorias identificados passaram por sucessivas revisões, sendo que, ao final, foram produzidos 44 códigos associados a 03 categorias: Estrutura da PTMOL, Dificuldade de uso da PTMOL e Percepção sobre a PTMOL.

Os procedimentos do GT permitiram alcançar uma análise aprofundada, comparando e analisando o relacionamento entre estes conceitos. Uma vez que a intenção deste estudo não é criar uma teoria, não foi realizada a codificação seletiva (terceira fase do método GT). As fases de codificação aberta e axial foram suficientes para entender aspectos positivos e negativos relacionados à utilidade, facilidade e dificuldade sobre o processo de aplicação da PTMOL. Além disso, foi possível obter a resposta para a questão de pesquisa do estudo após a execução das fases de codificação aberta e axial.

5.4.5 Resultados do terceiro estudo

5.4.5.1 Resultados qualitativos do grupo focal

Os códigos identificados nas transcrições foram agrupados de acordo com as suas propriedades, formando assim conceitos que representam categorias. Essas categorias foram analisadas em conjunto com outros pesquisadores com o objetivo de proporcionar uma maior clareza sobre o fenômeno de interesse. Foram produzidos 44 códigos associados a 03 categorias: Estrutura da PTMOL, Dificuldade de uso da PTMOL e Percepção sobre a PTMOL.

A Figura 5.13 apresenta o resultado da codificação para a categoria estrutura da PTMOL. Essa categoria demonstra os códigos derivados dos comentários dos participantes à respeito da organização do processo de aplicação da PTMOL. Os códigos são apresentados seguidos de dois números que representam respectivamente o grau de fundamentação (*groundedness*) e o de densidade teórica (*density*). O grau de fundamentação indica o número de citações com as quais o código está associado. O grau de densidade teórica aponta o número de relacionamentos do código com outros códigos. Além disso, existe a variação dimensional, que explicita as causas e efeitos para uma determinada categoria. As relações entre os códigos, denominadas de conectores, segundo Glaser (1992), podem ser definidas pelo próprio pesquisador. Para observar a variação dimensional foram propostos dois conectores: “é evidência de facilidade” e “é evidência de utilidade”. “É evidência de facilidade” mostra uma variação positiva para a estrutura da PTMOL, onde o processo de aplicação da linguagem é apontado como fácil de usar e aprender. “É evidência de utilidade” também apresenta uma variação positiva para a estrutura da PTMOL, exibindo os elementos e recursos da linguagem considerados adequados e úteis para uma modelagem de ameaças.

Com base na ilustração representada na Figura 5.13, em relação à estrutura da PTMOL, nota-se algumas evidências importantes que apontam para facilidade de uso da linguagem. Um exemplo dessas evidências pode ser visto a partir do código “possui uma estrutura para preenchimento de fácil compreensão”, código este relacionado a cinco comentários (grau de fundamentação do código é igual a cinco). Além disso, diversos outros comentários indicam evidências quanto à utilidade dos elementos e recursos da PTMOL. Um dos principais comentários ressaltados pelos participantes refere-se principalmente a capacidade de auto explicação das etapas de modelagem da linguagem. Os códigos “possui elementos que explicam bem a que se referem”, “ela é autoexplicativa” e “as categorias de ameaças são bem explicativas e com exemplos

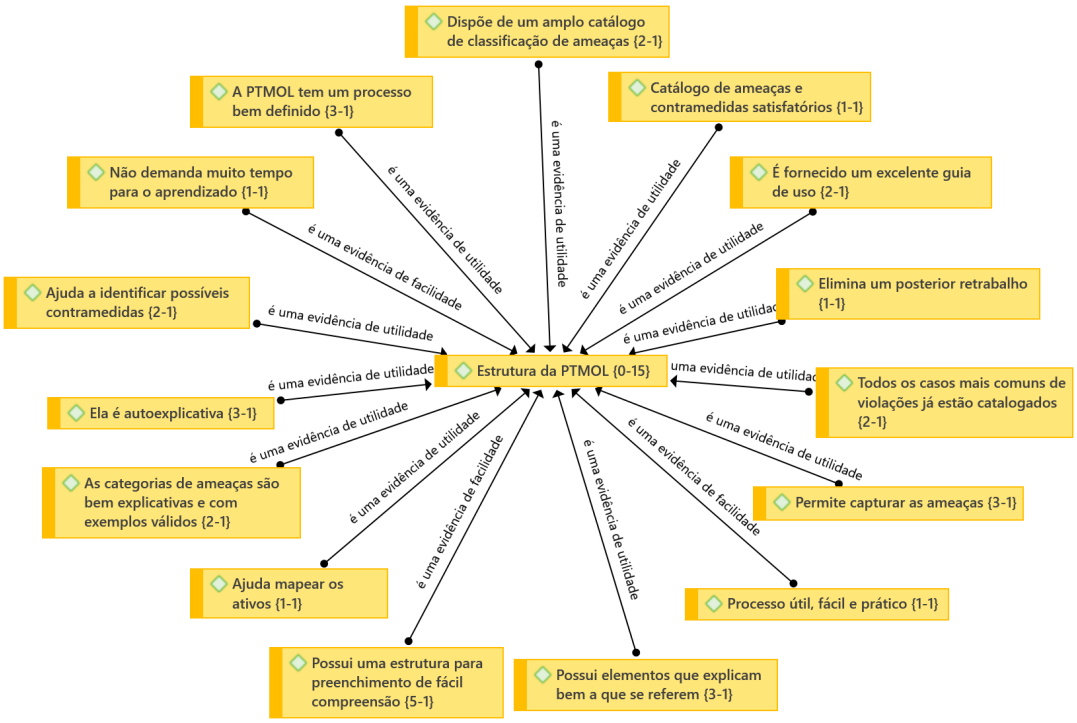


Figura 5.13: Códigos relacionados à percepção das equipes sobre a estrutura da PTMOL
Fonte: Próprio autor.

válidos" são demonstrações disso. Outros códigos apontam para a relevância dos recursos da PTMOL para um diagnóstico de ameaças de privacidade em RSOs, tais como "dispõe de um amplo catálogo de classificação de ameaças", "permite capturar ameaças" e "todos os casos mais comuns de violações já estão catalogados".

A Figura 5.14 apresenta as relações entre os códigos da categoria dificuldade de uso da PTMOL. Para observar a variação dimensional foi proposto apenas um conector: "é evidência de", no qual vincula códigos relacionados a aspectos que os participantes consideraram como dificuldades na aplicação da linguagem. Com base nos códigos representados na Figura 5.14, é possível observar que existem evidências de dificuldades em relação ao catálogo de ameaças da PTMOL, capturadas por meio dos códigos "é preciso reler várias vezes o catálogo de ameaças" e "é um pouco difícil lembrar do que a ameaça aborda apenas pelo nome". De fato, o catálogo de ameaças pode ou precisa ser consultado diversas vezes durante e etapa de identificação de ameaças, principalmente quando um designer não está familiarizado com alguns conceitos sobre elas. No entanto, essa questão não pode ser considerada como um problema, mas sim como um esforço inerente do procedimento de aplicação, que por ser uma modelagem conceitual em nível de design, exige um empenho maior por parte de quem está aplicando.

Pode-se observar também, por meio do grau de fundamentação igual a três, que os códigos "muitas informações para serem preenchidas" e "o processo de aplicação é

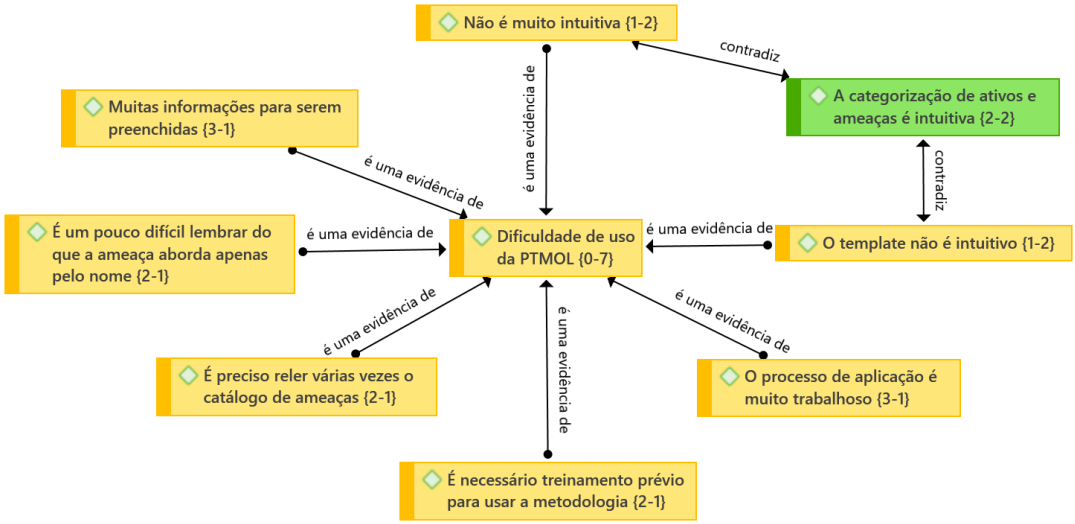


Figura 5.14: Códigos relacionados à percepção das equipes sobre dificuldade de uso da PTMOL

Fonte: Próprio autor.

muito trabalhoso" também indicam a necessidade de um esforço maior para aplicar a PTMOL. Essas evidências mostram que há um tempo e custo envolvidos no processo de aplicação da linguagem, mas que são fundamentais para garantir uma modelagem efetiva e completa de ameaças de privacidade em RSOs. Os códigos "não é muito intuitiva" e o "template não é intuitivo" são refutados pelo código "a categorização de ativos e ameaças é intuitiva".

Outro código como "é necessário treinamento prévio para usar a metodologia" pode ser enxergado como uma potencial dificuldade, mas não como uma limitação da proposta, uma vez que todo o procedimento metodológico quando aplicado pela primeira vez requer um treinamento prévio. Muito embora sabe-se que os autores da PTMOL não estarão presentes para conduzir treinamentos em tempo de uso, o objetivo da proposta é efetivamente tornar o processo de aplicação autoexplicativo, de modo que os futuros usuários da linguagem possam entendê-la sem um treinamento prévio. A categoria anterior, estrutura da PTMOL, indicou evidências relevantes sobre a capacidade de autoexplicação da linguagem.

Por fim, a Figura 5.15 apresenta as relações entre os códigos da categoria percepção sobre a PTMOL. Para observar a variação dimensional utilizou-se o conector original do GT, "é um tipo de" (*is a*), que conecta códigos relacionados à percepção dos participantes sobre aspectos gerais, positivos ou negativos, dos elementos e recursos da PTMOL. Alguns códigos apontam que o processo de aplicação da PTMOL pode ser complexo e genérico, "tem um processo complexo" e "pode ter um processo muito genérico". No entanto, ambos os códigos possuem grau de fundamentação baixo, com apenas 1 grau. Outros códigos como "são muitas classificações e detalhes", "há muitas

etapas no processo de coleta/análise de ativos e ameaças", "cada etapa tem muito conceito" e "é uma técnica extensa" não foram percebidos como problemas ou obstáculos referentes ao processo metodológico da PTMOL, mas sim como pontos importantes que demonstram que a linguagem produz uma orientação detalhada e completa para uma modelagem efetiva de ameaças de privacidade em nível de design.

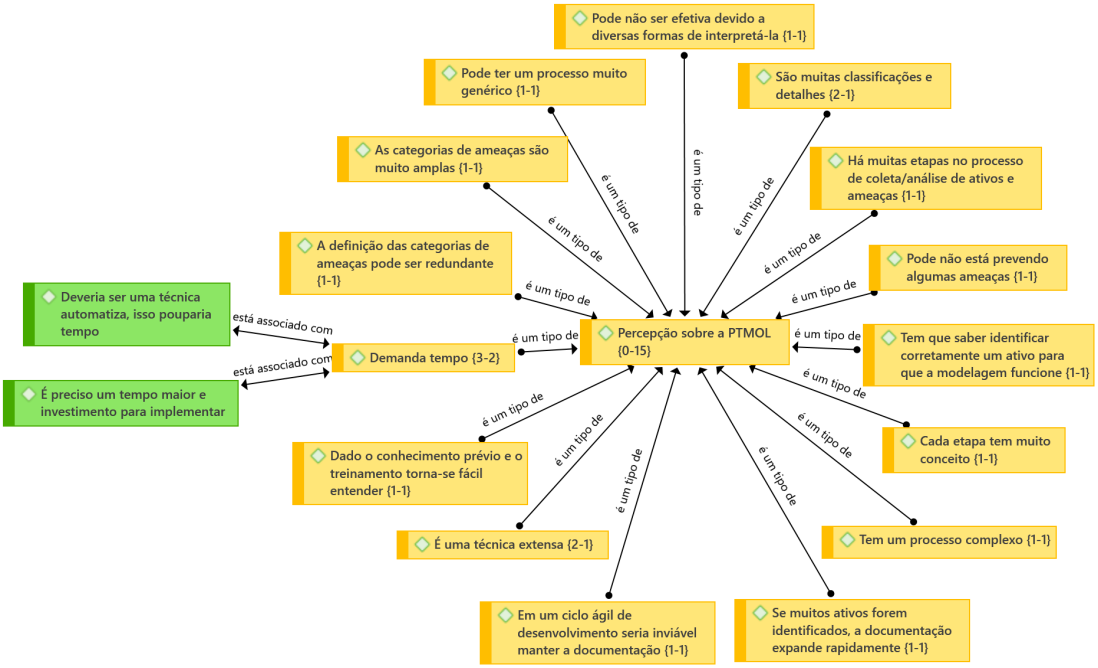


Figura 5.15: Códigos relacionados à percepção das equipes sobre a PTMOL
Fonte: Próprio autor.

Outros códigos como "em um ciclo ágil de desenvolvimento seria inviável manter a documentação" e "se muitos ativos foram identificados a documentação expande rapidamente" trazem um argumento interessante sobre fases do desenvolvimento de software em que a PTMOL não pode ser incorporada. Na sua concepção, a PTMOL é destinada para ser aplicada de modo a antecipar o diagnóstico e prevenção de ameaças de privacidade em nível de design de RSOs. De fato, em um ciclo de desenvolvimento ágil seria inviável utilizá-la, uma vez que um dos em valores ágeis, software funcionando é melhor do que documentação abrangente, distingue-se do propósito central da PTMOL, que dispõe de uma ampla documentação para mapear todos os cenários de ameaças que um usuário poderá estar potencialmente exposto. Por fim, códigos como "demanda tempo" ressalta novamente o tempo de esforço dedicado a aplicação da PTMOL e o código associado "deveria ser uma técnica automatizada, isso pouparia tempo" aponta a sugestão de uma ferramenta para automatizar o procedimento de aplicação da linguagem. Essa sugestão será analisada pelos autores como um incremento futuro à linguagem.

5.4.5.2 Resultados do *design rationale*

Após a finalização da sessão de coleta de dados por meio do grupo focal, os participantes se reuniram novamente com as suas equipes para registrar decisões sobre o processo de modelagem da PTMOL e sugestões de melhorias por meio do *design rationale*. Os dados analisados foram os relatórios fornecidos pelos participantes, que continham os registros do DR. Os relatórios foram examinados com três propósitos principais: (i) identificar os problemas comuns da modelagem de ameaças com a PTMOL; (ii) analisar os argumentos dos participantes sobre os problemas apontados; e (iii) identificar sugestões de melhorias. A Tabela 5.12 resume os principais problemas fornecidos pelas equipes, bem como possibilidades de melhorias.

Tabela 5.12: Problemas e possíveis soluções identificadas no *design rationale*

Questão/Problema	**Possível solução**	**Fonte**
As opções de fontes de vazamento são bastante genéricas e pode ser difícil associá-las a uma ameaça específica	Novos elementos poderiam ser adicionados, como atributos que detalhem mais as fontes de vazamento, de modo que seja possível diferenciá-las efetivamente	Equipe 1
A PTMOL não esclarece os padrões de preenchimento dos *templates* de modelagem.	A PTMOL poderia descrever as regras de preenchimento dos *templates* para não causar dúvidas no momento da modelagem	Equipe 2
Não possui uma ferramenta própria para modelagem de ameaças	Desenvolvimento de uma ferramenta de apoio à PTMOL que valide a sintaxe da linguagem e permita uma modelagem mais automatizada	Equipe 3
A associação da contramedida com a ameaça pode não estar efetivamente clara	Poderia indicar para cada ameaça listada no *template* de modelagem qual contramedida foi violada, assim fica mais claro pensar em estratégias de mitigação	Equipe 4

Com base nas informações apresentadas na Tabela 5.12, nota-se que foi possível elicitar problemas pontuais sobre a modelagem de ameaças com a PTMOL, que indicam necessidades de melhorias que poderiam ser implementadas com as possíveis soluções apontadas. Os problemas descritos e as possíveis soluções visam auxiliar os profissionais que utilizam a PTMOL a esclarecer dúvidas e minimizar dificuldades oriundas do uso da linguagem. Vale destacar que todos os argumentos foram sugeridos com base na experiência dos participantes durante o estudo de observação, o que reforça sua aplicabilidade. Cada necessidade de melhoria foi analisada e a viabilidade de implementá-la foi verificada com um segundo pesquisador. As melhorias viáveis foram realizadas, gerando a quarta versão da PTMOL, mostrada no Capítulo 4.

5.4.6 Melhorias na PTMOL após a execução do terceiro estudo

A análise dos dados qualitativos propiciou *insights* relevantes para melhorar a qualidade de uso da PTMOL, uma vez que tanto os dados coletados no grupo focal

como os registros fornecidos por meio do *design rationale* apontaram para problemas específicos sobre a linguagem. Estes problemas foram analisados e as melhorias viáveis foram implementadas, gerando a quarta versão da PTMOL. Inicialmente, foram analisados os códigos considerados evidências de dificuldade de aplicação do processo de modelagem de ameaças da PTMOL. Após a análise feita pelos pesquisadores especialistas na PTMOL, algumas adaptações foram realizadas no sentido de tornar os elementos da linguagem mais claros. Todas essas melhorias supracitadas foram incorporadas na versão 4.0 da PTMOL. As principais modificações implementadas incluem:

- Atualização nas definições de algumas ameaças do catálogo, de modo a torná-las mais claras e concisas e eliminar eventuais redundâncias.
- Criação de regra de preenchimento para os *templates* de modelagem.
- Eliminação de informações confusas.
- Descrição mais detalhada das fontes de vazamento

Um outro ponto limitativo observado no decorrer do estudo estava relacionado a etapa de identificação de contramedidas. Nessa etapa, o designer deve definir, como estratégias de mitigação, alertas de prevenção e contramedidas para cada ameaça listada no *template* de modelagem. Para tal, torna-se necessário consultar a taxonomia implementada com propriedades de privacidade e transformá-las em potenciais contramedidas. Apesar dos participantes, tanto do primeiro estudo quanto do segundo, terem indicado sugestões significativas para prevenir ou neutralizar os efeitos das ameaças de privacidade, percebeu-se que a associação da contramedida com a ameaça poderia não estar efetivamente clara.

Diante do exposto, foi implementada uma subetapa complementar à etapa de identificação de contramedidas. Antes de iniciar essa fase, o designer deverá indicar para cada ameaça listada no *template* de modelagem, qual propriedade de privacidade, presentes no próprio *template*, a mesma poderia violar. Essa forma de associação pode ser visualizada na Figura 5.16.

Após listar o conjunto de ameaças que podem ocorrer no sistema, o designer deverá indicar por meio de uma marcação de seleção (X) quais propriedades foram violadas. Para cada propriedade indicada como possivelmente violada, torna-se necessário transformar a propriedade em contramedida, de modo que esta possa prevenir ou dificultar os usos maliciosos previstos. Essa associação complementa o processo de modelagem e torna a etapa referida mais compreensível.

5.4.7 Limitações do terceiro estudo

Todo estudo possui limitações em seus resultados e elas precisam ser relatadas. Dentre as limitações deste estudo, destacamos três principais. A primeira está relacionada com o fato dos participantes serem estudantes de graduação e o estudo ser conduzido em um ambiente acadêmico. Sobre isto, Fernandez et al. (2012) afirmam que

Ameaça de privacidade 	Qual propriedade de privacidade pode ser violada?						
	Desvinculação	Anonimato	Negação plausível	Não detecção	Confidencialidade	Conscientização	Transparência
Ameaça 1	X					X	
Ameaça 2		X					
Ameaça 3			X				X
...				X		X	
Ameaça n		X			X		

Figura 5.16: Novo *template* para indicar propriedade de privacidade que pode ser violada por uma ameaça

estudantes que não têm experiência na indústria podem, no entanto, ter habilidades semelhantes aos profissionais menos experientes. Portanto, apesar da limitação imposta pela participação de estudantes no estudo e não de profissionais, acredita-se que os resultados encontrados não devem ser considerados inválidos.

Outra limitação pode estar relacionada à generalização dos resultados obtidos. A quantidade de participantes envolvidos no estudo não pode ser considerada como representativa, porém buscou-se mitigar essa ameaça pela obtenção e coleta de dados relevantes sobre o processo de aplicação da PTMOL. No entanto, não é possível afirmar que os resultados foram conclusivos, uma vez que por meio deste estudo foi feita apenas uma coleta de dados qualitativa.

Por fim, outra limitação trata-se da possibilidade do autor principal da pesquisa ter introduzido seu viés no processo de análise de dados. A este respeito, o processo de análise foi supervisionado por outro dois pesquisadores mais experientes. Esses pesquisadores revisaram e analisaram todos os resultados intermediários, tais como os dados qualitativos. Esse processo iterativo foi repetido até o final da coleta e análise de dados.

5.4.8 Conclusões do terceiro estudo

Mafra et al. (2006) afirmam que por meio de um estudo de observação é possível coletar dados sobre como uma determinada solução é aplicada. Desse modo, os pesquisadores podem adquirir uma compreensão refinada sobre a solução em análise, ao presenciarem potenciais dificuldades que os participantes possam apresentar. Diante disso, essa seção apresentou um estudo de observação com o objetivo de compreender o modo com que possíveis designers de sistemas aplicariam o processo de modelagem de ameaças da PTMOL. Os resultados do estudo foram positivos, uma vez que forneceram

insights relevantes para melhorar a qualidade da PTMOL.

Após a análise feita pelos pesquisadores especialistas na PTMOL, algumas atualizações e modificações foram realizadas no sentido de tornar os elementos e recursos da linguagem mais claros. Embora os resultados de uma única experiência não possam ser generalizados para outros contextos, acredita-se que os resultados qualitativos deste estudo de observação podem contribuir para melhorar o entendimento sobre o comportamento de designers novatos em modelagem de ameaças.

5.5 Quarto estudo: PTMOL comparada com técnica *ad hoc*

Os estudos anteriores focaram totalmente na caracterização da PTMOL, analisando os resultados da aplicação da linguagem por um conjunto de participantes que representavam potenciais usuários. Esses estudos forneceram evidências quantitativas e qualitativas de como a linguagem funcionaria em tempo de uso. Para este estudo final o foco é diferente, pois tem-se o propósito de examinar a confiabilidade dos resultados produzidos pelo processo de modelagem proposto pela PTMOL. Há a possibilidade de que o catálogo de ameaças implementado pela PTMOL seja limitado e, consequentemente, não esteja prevendo ameaças de privacidade importantes. Para checar essa hipótese, pedimos a sete especialistas em privacidade que realizassem uma análise de ameaças em uma RSO modelada por meio de um diagrama de classes. A condução e resultados do estudo serão descritos a seguir.

5.5.1 Caracterização do objeto de análise

Para aplicar a PTMOL em nível de design, torna-se necessária uma descrição geral dos recursos que permitem o usuário compartilhar dados no sistema ou dos recursos que informam como os dados serão coletados pela RSO. Com isso, pode-se utilizar como cenário para a modelagem de ameaças, modelos de tarefas e de interação, cenários, ou qualquer outra representação do sistema onde é possível compreender como funciona o compartilhamento, a coleta e o processamento dos dados do usuário.

Para o contexto desse estudo, utilizou-se um diagrama de classes que modelava uma RSO de compartilhamento de conteúdo. Essa escolha, diferente dos estudos anteriores, onde foram aplicados cenários de ameaças, deu-se para avaliar o comportamento de aplicação da PTMOL em um outro tipo de representação do sistema em nível de design. A Figura 5.17 apresenta o modelo utilizado como objeto de análise.

5.5.2 Especialistas em segurança e privacidade

Sete indivíduos especialistas em segurança e privacidade de sistemas foram convidados para participar da pesquisa. Os participantes receberam o diagrama de classes e foram solicitados a identificar o maior número possível de ameaças de privacidade para esse cenário. Os especialistas poderiam consultar os pesquisadores para

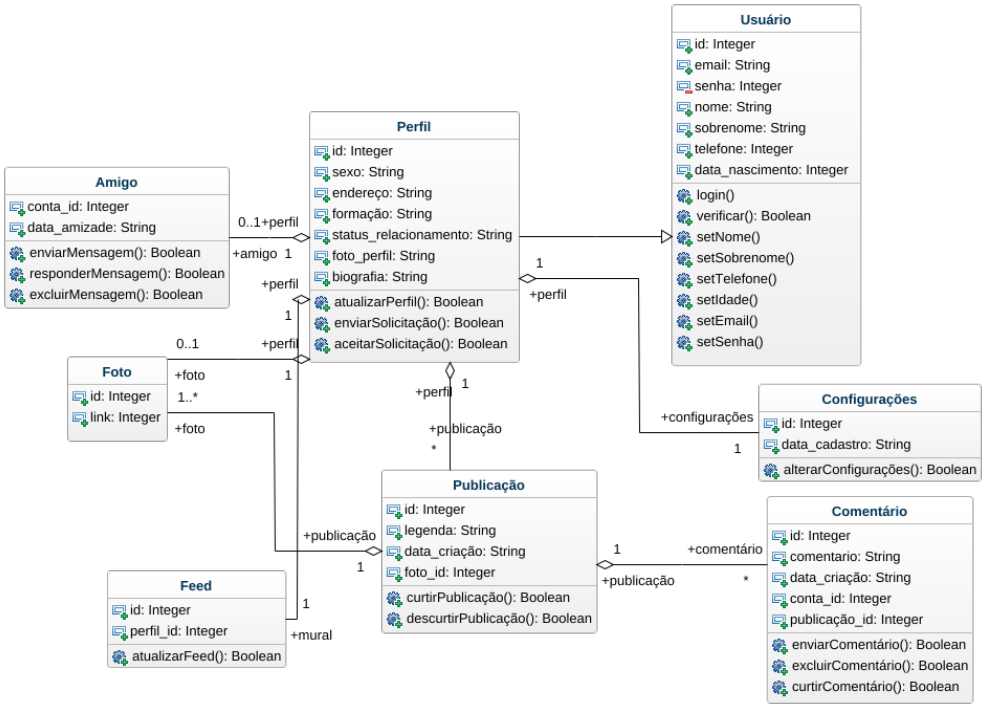


Figura 5.17: Diagrama de classes para análise do estudo
Fonte: Adaptado de GenMyModel

fazer perguntas específicas sobre o cenário. Para facilitar uma comparação uniforme, os especialistas foram solicitados a documentar as ameaças em um *template* (Figura 5.18), que exemplificava o nível de detalhes esperado deles na análise de ameaças. As instruções completas fornecidas aos especialistas podem ser consultadas no Apêndice D. Cada especialista trabalhou individualmente, ou seja, sem nenhum contato com outros, e utilizaram seus próprios conhecimentos (técnica *ad hoc*) para realizar a tarefa. É importante destacar que nenhum dos participantes conhecia a PTMOL, descartando assim qualquer possibilidade de viés.

Ao final da análise, que durou cerca de uma semana, os resultados foram recolhidos pelo autor da tese. Cada um dos especialistas teve que entregar um relatório que listava todas as ameaças identificadas no cenário em questão, que foram documentadas usando o modelo fornecido. Além disso, eles também discutiram individualmente seus resultados com o autor da tese, a fim de corrigir qualquer ambiguidade em seus relatórios. A Tabela 5.13 apresenta a caracterização dos participantes deste estudo, onde cada participante é relacionado com um ID, nível de formação e profissão.

Ativos	Ameaças de privacidade	Fontes de vazamento	Usos maliciosos
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	<Associar ameaça ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>
Ativo 2			
Ativo 3			
...			
Ativo n			

Figura 5.18: *Template* fornecido aos especialistas para identificação de ameaças *adhoc*
Fonte: Próprio autor.

Tabela 5.13: Caracterização dos participantes do estudo

ID	Formação	Profissão
P1	Mestre	Professora
P2	Mestre	Cybersecurity manager
P3	Especialista	Analista de TI
P4	Mestre	Professor
P5	Mestre	Servidor público
P6	Especialista	Professor
P7	Doutor	Cybersecurity manager

5.5.3 Especialistas em PTMOL

Três indivíduos são especialistas no uso da PTMOL: o autor desta tese e dois pesquisadores doutores, um da área de segurança e privacidade e outra da área de IHC e privacidade. Os três especialistas tinham que aplicar o processo de modelagem de ameaças da PTMOL para o mesmo diagrama de classes fornecido aos especialistas em privacidade. Somente a primeira e segunda etapa - identificação de ativos e de ameaças - da PTMOL foram realizadas, uma vez que o objetivo do estudo era comparar os resultados produzidos com a modelagem PTMOL em relação a uma identificação de ameaças *ad hoc*. O autor da tese realizou sua modelagem e apresentou os resultados aos seus coautores, que a revisaram. Após uma discussão conjunta para esclarecer qualquer discordância, os especialistas documentaram as ameaças identificadas em um relatório consolidado.

5.5.4 Hipóteses

Para o contexto deste estudo, buscou-se investigar a confiabilidade da PTMOL, avaliando se a linguagem não considerava alguma ameaça importante que, de forma *ad hoc*, poderia ser descoberta ou apontada por especialistas em privacidade. A partir

disso, o estudo foi conduzido para responder a seguinte questão de pesquisa: A PTMOL identifica menos ameaças de privacidade do que especialistas identificam utilizando uma técnica ad hoc? Os resultados fornecidos por meio da aplicação da PTMOL e da aplicação de uma técnica *ad hoc* são comparados para responder a questão de pesquisa. Com base nisso, formulou-se também a seguinte hipótese nula:

$$\mathrm{H}_0 : \mu\{\mathrm{Conf} = \frac{VP_{ptmol}}{VP_{ptmol} + FN_{ptmol}}\} < 0.80$$

Os falsos negativos (FN) representados na hipótese nula indicam as ameaças identificadas pelos especialistas em privacidade, que possivelmente não poderiam estar sendo consideradas no catálogo de ameaças da PTMOL. Pode-se observar que a definição de confiabilidade é semelhante ao conceito do *recall* utilizado nos estudos anteriores. Portanto, para consistência, utilizou-se o mesmo limite de 80%. Com isso, a expectativa é que a PTMOL encontre pelo menos 80% do número total de ameaças existentes no cenário avaliado.

5.5.5 Resultados do quarto estudo

Um oráculo (solução de referência) foi criado pelos especialistas da PTMOL com o propósito de fornecer uma estimativa de quantas ameaças de privacidade poderiam ser encontradas no cenário em análise. Os especialistas aplicaram a linguagem PTMOL no diagrama de classes, identificando um total de 40 ameaças, conforme apresentado na Tabela 5.14. Embora o oráculo seja a referência para a análise quantitativa do estudo, os participantes poderiam fazer suposições que divergiam do oráculo. Desse modo, a solução de referência é utilizada apenas como um guia para os avaliadores terem como base de comparação.

Tabela 5.14: Solução de referência indicando tipo e número de ameaças para o cenário do quarto estudo

Ameaças de privacidade	**Número de ameaças**
Clonagem de perfil	5
Ameaça à reputação	4
Cyberstalking	4
Divulgação de informação	9
Espionagem	1
Reconhecimento facial	2
Roubo de identidade	2
Inferência/Rastreamento	13
Gravação não autorizada	0
Total	**40**

A partir disso, o autor da tese e outro pesquisador examinaram cuidadosamente os relatórios produzidos pelos especialistas em privacidade, para identificar as ameaças

apontadas por eles e, posteriormente, comparar com o diagnóstico de ameaças produzidos pelos especialistas da PTMOL. A Tabela 5.15 apresenta o conjunto de ameaças registrado pelos participantes em seus relatórios, bem como a fonte da ameaça, ou seja, quem foi o participante que a indicou.

Tabela 5.15: Ameaças identificadas pelos participantes do estudo

Ameaças de privacidade	**Fonte**
Phishing	P3, P4, P7
Propaganda direcionada	P1, P7
Doxing	P7
Extorsão	P7
Elevação de privilégios	P5, P7
Divulgação de localização	P4, P5, P7
Extração de dados pessoais	P2, P6
Vazamento de informação	P2, P3, P4, P5, P6, P7
Acesso indevido	P2, P3, P6
Download indiscriminado de fotos	P5
Exposição de dados sensíveis	P1, P4

De uma perspectiva quantitativa, os especialistas que aplicaram a PTMOL identificaram 40 ameaças. Já os participantes do estudo encontraram, de forma *ad hoc*, 11 ameaças no cenário avaliado. No geral, constatou-se que as ameaças apontadas pelos participantes eram iguais ou semelhantes às ameaças identificadas pelos especialistas da PTMOL, embora estivessem descritas com nomenclaturas diferentes. Para estabelecer uma comparação válida e rastreável entre os resultados produzidos pelos participantes do estudo e pelos especialistas da PTMOL, associou-se cada ameaça indicada pelos participantes com uma ameaça correspondente da PTMOL, de modo que fosse possível checar a relação conceitual entre as ameaças. Esta análise pode ser vista na Tabela 5.16.

Tabela 5.16: Associação das ameaças apontadas pelos participantes especialistas com as ameaças da PTMOL

Ameaças/PTMOL	**Ameaças indicadas pelos especialistas**
Clonagem de perfil	
Ameaça à reputação	Elevação de privilégios, Extorsão
Cyberstalking	Extorsão
Divulgação de informação	Divulgação de localização, Exposição e Vazamento de dados, Doxing
Espionagem	
Reconhecimento facial	Download indiscriminado de fotos
Roubo de identidade	Phishing, Acesso indevido a dados privados
Inferência/Rastreamento	Propaganda direcionada, Extração de dados pessoais

A partir dessa análise, observa-se que todas as ameaças indicadas pelos especialistas em privacidade também foram indicadas pelos especialistas que aplicaram a

PTMOL e, portanto, todas estão previstas no catálogo de ameaças da linguagem. Isso indica que não houve incidência de falsos negativos, ou seja, ameaças que possivelmente não poderiam estar sendo consideradas pela PTMOL. Os resultados identificados indicam que, no cenário avaliado, havia um total de 40 ameaças (verdadeiros positivos - VP) e todas eram previstas pela PTMOL (0 falsos negativos - FN). Isso resulta em uma taxa de 100% de confiabilidade do processo de modelagem de ameaças da linguagem. Portanto, há evidências para refutar a hipótese nula, indicando que a PTMOL alcançou uma cobertura satisfatória comparativamente ao diagnóstico de ameaças produzido pelos participantes especialistas.

Embora os resultados de uma única experiência não possam ser generalizados para outros contextos, acredita-se que os resultados obtidos nesse estudo indicam que a PTMOL dispõe de um suporte relevante para especialistas e não especialistas atingirem um nível adequado em modelagem de ameaças de privacidade. Além disso, especialistas em privacidade podem utilizar a PTMOL como um suporte para evitar lacunas em suas atividades *ad hoc* de identificação de ameaças.

5.5.6 Limitações do quarto estudo

Todo estudo possui limitações em seus resultados e elas precisam ser relatadas. Dentre as limitações deste estudo, destacamos duas principais. A primeira está relacionada com as percepções dos especialistas, que podem ser tendenciosas em relação a suas próprias crenças, causando assim distorções na interpretação da realidade e consequente distorções nos resultados obtidos. Para reduzir essa limitação, buscou-se selecionar especialistas com maior experiência.

Por fim, outra limitação trata-se da possibilidade do autor principal da pesquisa ter introduzido seu viés no processo de análise de dados. A este respeito, o processo de análise foi supervisionado por outro dois pesquisadores mais experientes. Esses pesquisadores revisaram e analisaram todos os resultados intermediários. Esse processo iterativo foi repetido até o final da coleta e análise de dados.

5.6 Considerações do Capítulo

Este capítulo apresentou o processo de avaliação e evolução da PTMOL com base nos resultados de um conjunto de estudos empíricos. O planejamento, execução e resultados dos estudos foram apresentados. Foram conduzidos um estudo preliminar, um estudo de viabilidade, um estudo de observação e um estudo com especialistas. Todo o processo de evolução da PTMOL, e suas diferentes versões, pode ser consultado no Apêndice E.

O primeiro estudo foi conduzido com oito participantes para realizar os procedimentos de validade e confiabilidade da PTMOL e coletar oportunidades para o seu refinamento. Os resultados permitiram identificar melhorias a serem realizadas no processo de aplicação, como a necessidade de inserção ou adaptação de elementos para tornar o processo de modelagem de ameaças efetivamente mais claro. Com base nos

comentários dos participantes, a PTMOL foi refinada para atender às necessidades de melhorias identificadas e uma nova versão da linguagem foi criada.

O segundo estudo foi conduzido para avaliar a viabilidade da PTMOL como uma linguagem para a modelagem de ameaças de privacidade em nível de design. O estudo analisou os resultados da aplicação da PTMOL por um conjunto de participantes de um curso de Ciência da Computação. Os resultados do segundo estudo também apontaram indícios de que a PTMOL é aplicável até mesmo por profissionais não especialistas em privacidade, pois todos os participantes conseguiram mapear cenários de ameaças mesmo não tendo conhecimento técnico. Tal resultado foi um indício de que a PTMOL pode ser incorporada ao desenvolvimento de RSOs durante a fase de design e pode auxiliar designers de software na modelagem de ameaças, sem exigir um alto nível de especialidade na área de privacidade.

Uma vez que os resultados obtidos com os estudos anteriores indicaram a validade e viabilidade da PTMOL, realizou-se um terceiro estudo com o propósito de compreender de forma mais aprofundada o processo utilizado pelos designers ao aplicar a PTMOL durante uma modelagem de ameaças de privacidade, bem como identificar as situações nas quais as dificuldades no uso da linguagem poderiam ocorrer. Os resultados do estudo foram positivos, uma vez que forneceram *insights* relevantes para melhorar a qualidade da PTMOL. Após a análise feita pelos pesquisadores especialistas da PTMOL, algumas atualizações e modificações foram realizadas gerando a quarta versão da PTMOL

Os três estudos realizados forneceram evidências quantitativas e qualitativas de como a PTMOL funcionaria em tempo de uso. No entanto, um último estudo foi realizado com propósito de examinar a confiabilidade dos resultados produzidos pelo processo de modelagem proposto pela PTMOL. Com isso, o estudo foi realizado objetivando comparar os resultados produzidos com a modelagem PTMOL em relação a uma identificação de ameaças *ad hoc*. Os resultados obtidos nesse estudo indicaram que a PTMOL dispõe de um suporte relevante para especialistas e não especialistas atingirem um nível adequado em modelagem de ameaças de privacidade. Além disso, especialistas em privacidade podem utilizar a PTMOL como um suporte para evitar lacunas em suas atividades *ad hoc* de identificação de ameaças.

Capítulo 6

Conclusões e Perspectivas Futuras

Este capítulo apresenta as conclusões desta pesquisa, resumindo sua motivação, proposta e principais contribuições. As perspectivas futuras fornecem direcionamento para que seja dada a continuidade a este trabalho de pesquisa.

6.1 Conclusões

À medida que os usuários confiam cada vez mais nas RSOs para suas atividades de comunicação e interação, o processamento de dados pessoais por meio dessas redes pode expor os usuários a diversos tipos de ameaças de privacidade. Antecipar a preocupação com a privacidade para as etapas que antecedem o desenvolvimento de RSOs é uma estratégia promissora para tratar a proteção de dados pessoais ainda em nível de design. Esse interesse aumenta a credibilidade do uso de metodologias de modelagem de ameaças e traz oportunidades para o desenvolvimento de novas soluções que abordam esse tema.

Diante disso, este trabalho teve como objetivo central apoiar a modelagem de ameaças em RSOs, com foco específico na privacidade do usuário. Para atingir este propósito, definiu-se a PTMOL *(Privacy Threat Modeling Language)*, uma linguagem de apoio ao design de ameaças de privacidade orientada a RSOs. Esta linguagem foi desenvolvida a partir de evidências coletadas na literatura e foi avaliada empiricamente por meio de quatro estudos.

Ao longo desta pesquisa buscou-se aplicar os conceitos recomendados pelo o ciclo de *Design Science Research* (DSR), que estabelece as etapas de uma pesquisa para resolver um problema por meio da criação de uma solução (artefato). As principais etapas adotadas foram: (i) investigação do problema, onde foi realizado um mapeamento sistemático; (ii) objetivo da solução, onde um artefato inicial foi concebido; (iii) projeto e desenvolvimento, onde definiu-se a PTMOL; e (iv) avaliação, a qual foi realizada por meio de estudos empíricos.

Inicialmente, um protocolo para a condução de um mapeamento sistemático foi elaborado e executado, objetivando compreender o estado da arte sobre as principais ameaças de privacidade específicas para o contexto de RSOs e soluções para mitigá-las. A partir disso, identificou-se uma lacuna sobre propostas de modelagem de ameaças de privacidade específicas para tratar a proteção de dados do usuário em RSOs. Baseado nisso, buscou-se a proposição de uma solução que suprisse essa lacuna. Uma análise sobre os elementos que integravam a metodologia de modelagem de ameaças foi realizada em termos de adequação ao contexto de privacidade em RSOs. Com base nos elementos previamente definidos, uma nova linguagem para modelagem de ameaças foi elaborada, a qual foi denominada PTMOL.

6.2 Principais Contribuições

1. *Privacy Threat Modeling Language (PTMOL)*. A PTMOL é uma solução para a modelagem de ameaças de privacidade com foco na proteção de dados do usuário. A PTMOL pode ser incorporada ao desenvolvimento de RSOs durante a fase de design, possibilitando que designers de sistemas prevejam possíveis ameaças de privacidade, suas consequências e como elas podem ser mitigadas.

Para apoiar o processo de modelagem de ameaças, a PTMOL dispõe de um conjunto de recursos. O primeiro recurso estabelecido é o catálogo de ameaças, o qual descreve as ameaças mais críticas para a privacidade do usuário. Esse catálogo de ameaças é um recurso de grande valor, pois ajuda o designer a refletir sobre quais cenários de ameaça um usuário está potencialmente exposto. Um segundo recurso previsto é a taxonomia de contramedidas, que pode ser utilizada para prevenir ou mitigar os efeitos das ameaças. Após entender um possível cenário de ameaças ao qual o usuário poderá está exposto, a PTMOL possibilita que o designer defina trechos da sua modelagem de ameaças a partir de padrões, ou *templates,* integrados à linguagem, de modo que sua compreensão sobre o problema e possíveis soluções se amplie.

O processo de aplicação da PTMOL permite dividir um processo complexo em tarefas menores, facilitando a identificação de todo o cenário de ameaças. Assim, para iniciar a modelagem de ameaças via *template*, o designer terá que seguir um conjunto atividades para identificar: (i) o que é necessário proteger do usuário (ativos), (ii) quais eventos indesejáveis (ameaças) podem ocorrer e colocar em risco os ativos do usuário; e (iii) quais estratégias adotar (contramedidas) para prevenir ou mitigar os efeitos das ameaças aos dados do usuário. Os principais artigos sobre a PTMOL foram publicados em:

- Rodrigues, A., Villela, M. L., Feitosa, E. PTMOL: A suitable approach for modeling privacy threats in online social networks. In *Proceedings of the 21st Brazilian Symposium on Human Factors in Computing Systems*. 2022. p. 1-12.

- Rodrigues, A., Villela, M. L., Feitosa, E. Privacy Threat MOdeling Language. 2022. *IEEE Access*.

2. Validação empírica da PTMOL. Durante o desenvolvimento da PTMOL, testamos a linguagem por meio de um conjunto de estudos empíricos. É necessário que uma solução direcionada para ser aplicada em tempo de design seja executada pelos seus potenciais usuários, ou seja, não apenas a solução em si, mas também o papel dos indivíduos deve ser levado em consideração durante a validação. Nesse sentido, avaliamos empiricamente a PTMOL para entender como ela é aprendida e aplicada em tempo de uso.

Inicialmente, dois estudos experimentais foram executados para avaliar a completude, a corretude, a produtividade, a facilidade de uso, utilidade, satisfação percebida e intenção de uso futuro da PTMOL. Como a PTMOL pode ser utilizada durante a fase de design do ciclo de vida do desenvolvimento de software, a avaliação levou em consideração a perspectiva de potenciais designers de sistemas. A análise quantitativa dos estudos indicou bons resultados para a corretude e completude do processo de modelagem de ameaças da PTMOL. Os resultados para os indicadores de utilidade e facilidade de uso foram, no geral, positivos. Por se tratar de uma modelagem conceitual destinada para ser aplicada em nível de design, os resultados produzidos pela equipe de design precisam ser detalhados o suficiente para garantir uma interpretação de qualidade do cenário de ameaça sob análise.

Além disso, os resultados do segundo estudo também apontaram indícios de que a PTMOL é aplicável até mesmo por profissionais não especialistas em privacidade, pois todos os participantes conseguiram mapear cenários de ameaças mesmo não tendo conhecimento técnico. Isso pode ser um indicador de que a PTMOL pode ser incorporada ao desenvolvimento de RSOs durante a fase de design e pode auxiliar designers de software na modelagem de ameaças, sem exigir um alto nível de especialidade na área de privacidade.

Uma vez que os resultados obtidos com os estudos anteriores indicaram a validade e viabilidade da PTMOL, realizou-se um terceiro estudo com o objetivo de compreender o modo com que possíveis designers de sistemas aplicariam o processo de modelagem de ameaças da PTMOL. Os resultados do estudo foram positivos, uma vez que forneceram *insights* relevantes para melhorar a qualidade da PTMOL.

Por fim, um último estudo foi realizado com propósito de examinar a confiabilidade dos resultados produzidos pelo processo de modelagem proposto pela PTMOL. Para isso, a PTMOL teve que competir com especialistas em privacidade. Nesse sentido, sete especialistas foram solicitados a detectar ameaças de privacidade usando seus próprios procedimentos e esses resultados foram comparados com os da PTMOL. Os resultados obtidos nesse estudo indicaram que a PTMOL alcançou uma cobertura satisfatória comparativamente ao diagnóstico de ameaças produzido pelos participantes especialistas, atingindo 100% de confiabilidade. Além disso, especialistas em privacidade podem utilizar a PTMOL como um suporte para evitar lacunas em suas atividades *ad hoc* de identificação de ameaças.

3. Melhorias na PTMOL fundamentadas em evidência empírica. Os resultados dos estudos empíricos possibilitaram coletar oportunidades de melhorias e refinamento para o processo de modelagem da PTMOL. O elemento "controle" da composição de elementos da PTMOL foi retirado, deixando somente os elementos "alerta de prevenção" e "contramedidas" como estratégias de mitigação. O elemento "ações do atacante", que permitia o designer criar um racional sobre as possíveis ações que um agente malicioso pode realizar quando estiver de posse dos ativos do usuário, foi renomeado para usos maliciosos previstos. Na etapa de classificação de ativos, percebeu-se que o *template* de classificação de ativos compartilhados pelo usuário não previa a classificação dos ativos coletados e processados pelo sistema, que não necessariamente são divulgados pelo usuário, mas que são coletados e combinados para gerar outras informações pessoais. Com isso, criou-se um segundo *template* para também viabilizar a classificação de ativos coletados pelo sistema.

Outra mudança importante foi no catálogo de ameaças da PTMOL. Durante os estudos, percebeu-se que nem sempre os participantes estavam familiarizados com os conceitos generalistas de um tipo específico de ameaça. Com isso, foi inserido um resumo sobre os possíveis impactos de tais ameaças para a privacidade do usuário, de modo que fosse possível compreender a gravidade da ameaça.

Inserimos também o elemento "fontes de vazamento", o qual foi classificado em 4 tipos: (i) membro malicioso; (ii) provedor de serviços; (iii) aplicações terceirizadas; e (iv) fontes externas. Indicar a fonte responsável pela ameaça traz uma complementação ao processo de modelagem da PTMOL e ajuda a refletir de forma mais correta sobre os usos maliciosos que aquela determinada fonte poderá produzir. Também foi implementada uma subetapa complementar a etapa de identificação de contramedidas, para que fosse possível indicar para cada ameaça listada no *template* de modelagem, qual propriedade de privacidade, presentes no próprio *template*, a mesma poderia violar. Por fim, outros incrementos foram realizados como atualização nas definições de algumas ameaças do catálogo, de modo a torná-las mais claras e concisas e eliminar eventuais redundâncias, criação de regra de preenchimento para os *templates* de modelagem, e eliminação de informações confusas e descrição mais detalhada das fontes de vazamento.

6.3 Limitações da Tese

As principais limitações deste trabalho estão relacionadas, principalmente, ao tamanho da amostra. Nos estudos realizados, a principal dificuldade era tentar selecionar um número ideal de participantes heterogêneos como amostra. Ressalta-se que o tamanho da amostra é um problema conhecido em estudos IHC e Engenharia de Software (Fernandez et al., 2012). O pequeno número de participantes selecionados para os estudos pode não ser o ideal do ponto de vista estatístico, mas do ponto de vista qualitativo, os resultados dos estudos foram satisfatórios e viabilizaram oportunidades de melhorias e refinamentos para aumentar a qualidade da PTMOL.

6.4 Perspectivas Futuras

Os resultados obtidos abrem novas perspectivas de pesquisa, que podem ser exploradas em trabalhos futuros. Alguns dos trabalhos futuros são descritos a seguir:

- **Avaliação das melhorias**. As mudanças implementadas na PTMOL foram baseadas nos resultados dos estudos empíricos, que possibilitaram melhorar a qualidade geral da linguagem. Como perspectivas futuras, destacamos a continuidade de estudos empíricos para avaliar a nova versão da PTMOL com a finalidade de ampliar a confiabilidade dos resultados obtidos. Um novo estudo pode ser realizado com condições experimentais semelhantes ao dos anteriores, de modo a avaliar a versão aprimorada da PTMOL. Esses resultados podem então ser comparados com os anteriores para determinar se as mudanças realmente introduzem melhorias para nossas questões de pesquisa. Outra validação interessante seria avaliar ainda mais a PTMOL em um ambiente profissional. Até o presente momento da pesquisa, os participantes dos estudos eram em sua maioria estudantes. No entanto, como as melhorias propostas resultaram em uma versão mais completa da PTMOL, seria interessante examinar como os profissionais em um ambiente industrial percebem o uso da linguagem.

- **Manutenção do catálogo de ameaças**. Conforme mencionado anteriormente, as preocupações com a privacidade continuam evoluindo e a manutenção do catálogo de ameaças será necessária. De fato, as ameaças devem ser atualizadas regularmente com base em pesquisas na literatura ou evidências empíricas. Embora não houve nenhum feedback sobre a inserção de novas ameaças por meio dos estudos empíricos, isso não significa que as ameaças não possam sofrer uma atualização.

- **Suporte ferramental**. À medida que a PTMOL ganhe algum nível de popularidade, pode ser benéfico adicionar algum suporte ferramental para atingir um público ainda maior. A ferramenta pode, semelhante à ferramenta de modelagem de ameaças da Microsoft, fornecer suporte para gerar automaticamente os *templates* de modelagem e posteriormente gerar um modelo automático de ameaças. O catálogo de ameaças pode, por exemplo, ser interativo.

- **LGPD, termos de uso e políticas de privacidade**. Devido aos avanços das RSOs, torna-se cada vez mais fácil coletar dados pessoais de usuários, como é feito por grandes empresas como Google ou Facebook. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, é a legislação brasileira que regula a proteção de dados e a privacidade de todos os cidadãos do Brasil. Com isso, os desenvolvedores de software enfrentam inúmeros desafios, desde entender o que essa lei exige de seu software até adaptar seus processos de desenvolvimento para considerar os requisitos de privacidade e proteção de dados exigidos. Um potencial trabalho futuro seria investigar como o processo de modelagem de ameaças de

privacidade da PTMOL pode contribuir para a conformidade de termos de uso, políticas de privacidade e com a LGPD.

Conforme demonstrado nesta tese, a PTMOL é uma linguagem pronta para ser incorporada no desenvolvimento de RSOs na fase de design. Essas perspectivas futuras podem contribuir para melhorar a qualidade do processo de modelagem de ameaças de privacidade da PTMOL, tornanda-o ainda mais estável e pronta para ser aplicada em tempo de design.

Referências Bibliográficas

J. Abawajy, M. Ninggal, and T. Herawan. Privacy preserving social network data publication. *IEEE Communications Surveys and Tutorials*, 18(3):1974–1997, 2016a. doi: 10.1109/COMST.2016.2533668. cited By 37.

J. Abawajy, M. Ninggal, Z. Aghbari, A. Darem, and A. Alhashmi. Privacy threat analysis of mobile social network data publishing. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 239:60–68, 2018. doi: 10.1007/978-3-319-78816-6_5. cited By 0.

J. H. Abawajy, M. I. H. Ninggal, and T. Herawan. Privacy preserving social network data publication. *IEEE communications surveys & tutorials*, 18(3):1974–1997, 2016b.

Y. Abid, A. Imine, and M. Rusinowitch. Online testing of user profile resilience against inference attacks in social networks. *Communications in Computer and Information Science*, 909:105–117, 2018a. doi: 10.1007/978-3-030-00063-9_12. cited By 0.

Y. Abid, A. Imine, and M. Rusinowitch. Online testing of user profile resilience against inference attacks in social networks. In *European Conference on Advances in Databases and Information Systems*, pages 105–117. Springer, 2018b.

C. C. Aggarwal. An introduction to social network data analytics. In *Social network data analytics*, pages 1–15. Springer, 2011.

C. Akcora, B. Carminati, and E. Ferrari. Privacy in social networks: How risky is your social graph? pages 9–19, 2012. doi: 10.1109/ICDE.2012.99. cited By 38.

A. Aktypi, J. Nurse, and M. Goldsmith. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. volume 2017-January, pages 1–11, 2017. doi: 10.1145/3137616.3137617. cited By 6.

H. Al-Asmari and M. Saleh. A conceptual framework for measuring personal privacy risks in facebook online social network. 2019a. doi: 10.1109/ICCISci.2019.8716477. cited By 0.

H. A. Al-Asmari and M. S. Saleh. A conceptual framework for measuring personal privacy risks in facebook online social network. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6. IEEE, 2019b.

J. Alemany, E. Del Val, J. Alberola, and A. Garcia-Fornes. Metrics for privacy assessment when sharing information in online social networks. *IEEE Access*, 7:143631–143645, 2019a. doi: 10.1109/ACCESS.2019.2944723. cited By 0.

J. Alemany, E. del Val, J. Alberola, and A. García-Fornes. Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human Computer Studies*, 129:27–40, 2019b. doi: 10.1016/j.ijhcs.2019.03.008. cited By 0.

I. Alexander. Misuse cases: Use cases with hostile intent. *IEEE software*, 20(1):58–66, 2003.

S. Ali, N. Islam, A. Rauf, I. U. Din, M. Guizani, and J. J. Rodrigues. Privacy and security issues in online social networks. *Future Internet*, 10(12):114, 2018.

S. Ali, A. Rauf, N. Islam, and H. Farman. A framework for secure and privacy protected collaborative contents sharing using public osn. *Cluster Computing*, 22:7275–7286, 2019. doi: 10.1007/s10586-017-1236-2. cited By 0.

F. Alrayes, A. Abdelmoty, W. El-Geresy, and G. Theodorakopoulos. Modelling perceived risks to personal privacy from location disclosure on online social networks. *International Journal of Geographical Information Science*, 34(1):150–176, 2020. doi: 10.1080/13658816.2019.1654109. cited By 0.

I. Altman. The environment and social behavior: Privacy, personal space, territory, and crowding. 1975.

S. Barbosa and B. Silva. *Interação humano-computador*. Elsevier Brasil, 2010.

V. R. Basili. The role of experimentation in software engineering: past, current, and future. In *Proceedings of IEEE 18th International Conference on Software Engineering*, pages 442–449. IEEE, 1996.

V. R. Basili and H. D. Rombach. The tame project: Towards improvement-oriented software environments. *IEEE Transactions on software engineering*, 14(6):758–773, 1988.

J. Biega, I. Mele, and G. Weikum. Probabilistic prediction of privacy risks in user search histories. pages 29–36, 2014. doi: 10.1145/2663715.2669609. cited By 5.

J. A. Biega, K. P. Gummadi, I. Mele, D. Milchevski, C. Tryfonopoulos, and G. Weikum. R-susceptibility: An ir-centric approach to assessing privacy risks for users in online communities. In *Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval*, pages 365–374, 2016.

L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed, A. Torasso, and R. Pensa. A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies*, 12(4):456–469, 2019. doi: 10.1109/TLT.2018.2881193. cited By 1.

D. M. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1):210–230, 2007.

H. Briola, G. Drosatos, G. Stamatelatos, S. Gyftopoulos, and P. S. Efraimidis. Privacy leakages about political beliefs through analysis of twitter followers. In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pages 16–21, 2018.

I. Casas, J. Hurtado, and X. Zhu. Social network privacy: Issues and measurement. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9419:488–502, 2015. doi: 10.1007/978-3-319-26187-4_44. cited By 2.

A. Cavoukian et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5:12, 2009.

M. Cheung and J. She. Evaluating the privacy risk of user-shared images. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 12(4s):1–21, 2016.

J. Corbin and A. Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

S. De and A. Imine. To reveal or not to reveal: Balancing user-centric social benefit and privacy in online social networks. pages 1157–1164, 2018a. doi: 10.1145/3167132.3167258. cited By 3.

S. De and A. Imine. Privacy scoring of social network user profiles through risk analysis. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10694 LNCS:227–243, 2018b. doi: 10.1007/978-3-319-76687-4_16. cited By 0.

B. B. N. de França, T. V. Ribeiro, P. S. M. dos Santos, and G. H. Travassos. Using focus group in software engineering: lessons learned on characterizing software technologies in academia and industry. In *CIbSE*, page 351, 2015.

S. Deliri and M. Albanese. Security and privacy issues in social networks. In *Data Management in Pervasive Systems*, pages 195–209. Springer, 2015.

T. Denning, B. Friedman, and T. Kohno. The security cards: A security threat brainstorming toolkit. *Univ. of Washington, http://securitycards. cs. washington. edu*, 2013.

V. J. Derlega and A. L. Chaikin. Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3):102–115, 1977.

C. Dong and B. Zhou. Privacy inference analysis on event-based social networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10047 LNCS:421–438, 2016. doi: 10.1007/978-3-319-47874-6_29. cited By 0.

A. Dresch, D. P. Lacerda, and P. A. C. Miguel. Uma análise distintiva entre o estudo de caso, a pesquisa-ação e a design science research. *Revista Brasileira de Gestão de Negócios*, 17:1116–1133, 2015.

S. Du, X. Li, J. Zhong, L. Zhou, M. Xue, H. Zhu, and L. Sun. Modeling privacy leakage risks in large-scale social networks. *IEEE Access*, 6:17653–17665, 2018.

F. Erlandsson, M. Boldt, and H. Johnson. Privacy threats related to user profiling in online social networks. pages 838–842, 2012. doi: 10.1109/SocialCom-PASSAT.2012.16. cited By 11.

A. Fernandez, S. Abrahão, E. Insfran, and M. Matera. Further analysis on the validation of a usability inspection method for model-driven web development. In *Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement*, pages 153–156, 2012.

N. Ferreyra, R. Meis, and M. Heisel. Should user-generated content be a matter of privacy awareness? a position paper. volume 3, pages 212–216, 2017. cited By 2.

N. E. D. Ferreyra, R. Meis, and M. Heisel. At your own risk: shaping privacy heuristics for online self-disclosure. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–10. IEEE, 2018.

R. Fogues, J. Such, A. Espinosa, and A. Garcia-Fornes. Open challenges in relationship-based privacy mechanisms for social network services. *International Journal of Human-Computer Interaction*, 31(5):350–370, 2015. doi: 10.1080/10447318.2014.1001300. cited By 30.

B. G. Glaser. *Basics of grounded theory analysis: Emergence vs forcing.* Sociology press, 1992.

B. G. Glaser, A. L. Strauss, and E. Strutzel. The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17(4):364, 1968.

L. Gonzalez, P. Wightman Rojas, M. Labrador, et al. A survey on privacy in location-based services. *Ingeniería y Desarrollo*, 32(2):314–343, 2014.

A. R. Hevner, S. T. March, J. Park, and S. Ram. Design science in information systems research. *MIS quarterly*, pages 75–105, 2004.

O. Jaafor and B. Birregah. Multi-layered graph-based model for social engineering vulnerability assessment. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 1480–1488. IEEE, 2015.

O. Jaafor, B. Birregah, C. Perez, and M. Lemercier. Privacy threats from social networking service aggregators. pages 30–37, 2015. doi: 10.1109/CTC.2014.12. cited By 2.

L. Jin, X. Long, and J. Joshi. Towards understanding residential privacy by analyzing users' activities in foursquare. pages 25–32, 2012. doi: 10.1145/2382416.2382428.

S. Joyee De and A. Imine. On consent in online social networks: Privacy impacts and research directions (short paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11391 LNCS:128–135, 2019. doi: 10.1007/978-3-030-12143-3_11. cited By 0.

S. Kavianpour, Z. Ismail, and A. Mohtasebi. Effectiveness of using integrated algorithm in preserving privacy of social network sites users. *Communications in Computer and Information Science*, 167 CCIS(PART 2):237–249, 2011. doi: 10.1007/978-3-642-22027-2_20. cited By 0.

R. Khan, K. McLaughlin, D. Laverty, and S. Sezer. Stride-based threat modeling for cyber-physical systems. In *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, pages 1–6. IEEE, 2017.

H. H. Khondker. Role of the new media in the arab spring. *Globalizations*, 8(5):675–679, 2011.

K. H. Kim, K. Kim, and H. K. Kim. Stride-based threat modeling and dread evaluation for the distributed control system in the oil refinery. *ETRI Journal*, 2021.

B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. 2007.

B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, and S. Linkman. Systematic literature reviews in software engineering–a tertiary study. *Information and software technology*, 52(8):792–805, 2010.

B. A. Kitchenham, D. Budgen, and O. P. Brereton. Using mapping studies as the basis for further research–a participant-observer case study. *Information and Software Technology*, 53(6):638–651, 2011.

A. Korolova, R. Motwani, S. U. Nabar, and Y. Xu. Link privacy in social networks. In *Proceedings of the 17th ACM conference on Information and knowledge management*.

M. Kosinski, D. Stillwell, and T. Graepel. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the national academy of sciences*, 110(15):5802–5805, 2013.

H. Kumar, S. Jain, and R. Srivastava. Risk analysis of online social networks. pages 846–851, 2017. doi: 10.1109/CCAA.2016.7813833. cited By 1.

D. P. Lacerda, A. Dresch, A. Proença, and J. A. V. Antunes Júnior. Design science research: método de pesquisa para a engenharia de produção. *Gestão & produção*, 20:741–761, 2013.

O. Laitenberger and H. M. Dreyer. Evaluating the usefulness and the ease of use of a web-based inspection data collection tool. In *Proceedings Fifth International Software Metrics Symposium. Metrics (Cat. No. 98TB100262)*, pages 122–132. IEEE, 1998.

C. Laorden, B. Sanz, G. Alvarez, and P. G. Bringas. A threat model approach to threats and vulnerabilities in on-line social networks. In *Computational Intelligence in Security for Information Systems 2010*, pages 135–142. Springer, 2010.

J. Lazar and S. D. Barbosa. Introduction to human-computer interaction. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1202–1204, 2017.

J. Lee. Design rationale systems: understanding the issues. *IEEE expert*, 12(3):78–85, 1997.

J. Li. A privacy preservation model for health-related social networking sites. *Journal of Medical Internet Research*, 17(7), 2015. doi: 10.2196/jmir.3973. cited By 14.

Y. Li, Y. Li, Q. Yan, and R. Deng. Privacy leakage analysis in online social networks. *Computers and Security*, 49:239–254, 2015. doi: 10.1016/j.cose.2014.10.012.

S. N. Mafra, R. F. Barcelos, and G. H. Travassos. Aplicando uma metodologia baseada em evidência na definição de novas tecnologias de software. In *Anais do XX Simpósio Brasileiro de Engenharia de Software*, pages 239–254. SBC, 2006.

S. Mahmood. New privacy threats for facebook and twitter users. pages 164–169, 2012. doi: 10.1109/3PGCIC.2012.46. cited By 10.

A. B. d. S. Marques et al. Usinn: um modelo de interação e navegação orientado à usabilidade. 2017.

N. R. Mead, F. Shull, K. Vemuru, and O. Villadsen. A hybrid threat modeling method. *Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002*, 2018.

E. Mendes. A systematic review of web engineering research. In *2005 International Symposium on Empirical Software Engineering, 2005.*, pages 10–pp. IEEE, 2005.

Microsoft. Threat modeling. urlhttps://msdn.microsoft.com/ en-us/library/ff648644.aspx, 2003.

M. C. d. S. Minayo. Pesquisa social: teoria, método e criatividade. In *Pesquisa social: teoria, método e criatividade*, pages 80–80. 1994.

M. Ninggal and J. Abawajy. Privacy threat analysis of social network data. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7017 LNCS(PART 2):165–174, 2011. doi: 10.1007/978-3-642-24669-2_16. cited By 6.

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

D. L. Olson and D. Delen. *Advanced data mining techniques*. Springer Science & Business Media, 2008.

S. Oukemeni, H. Rifà-Pous, and J. M. M. Puig. Privacy analysis on microblogging online social networks: a survey. *ACM Computing Surveys (CSUR)*, 52(3):1–36, 2019.

P. Panagiotopoulos, A. Z. Bigdeli, and S. Sams. Citizen–government collaboration on social media: The case of twitter in the 2011 riots in england. *Government information quarterly*, 31(3):349–357, 2014.

M. C. F. Pelicioni et al. A utilização do grupo focal como metodologia qualitativa na promoção da saúde. *Revista da Escola de Enfermagem da USP*, 35:115–121, 2001.

R. Pensa and G. Di Blasi. A privacy self-assessment framework for online social networks. *Expert Systems with Applications*, 86:18–31, 2017. doi: 10.1016/j.eswa.2017.05.054. cited By 10.

K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson. Systematic mapping studies in software engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*, pages 1–10, 2008.

S. Petronio. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

M. Petticrew and H. Roberts. *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons, 2008.

A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010.

B. Potteiger, G. Martins, and X. Koutsoukos. Software and attack centric integrated threat modeling for quantitative risk assessment. In *Proceedings of the Symposium and Bootcamp on the Science of Security*, pages 99–108, 2016.

S. Puglisi, D. Rebollo-Monedero, and J. Forné. On the anonymity risk of time-varying user profiles. *Entropy*, 19(5):1–16, 2017. doi: 10.3390/e19050190. cited By 0.

K. Rannenberg. Iso/iec standardization of identity management and privacy technologies. *Datenschutz und Datensicherheit-DuD*, 35(1):27–29, 2011.

S. Rathore, P. Sharma, V. Loia, Y.-S. Jeong, and J. Park. Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421:43–69, 2017. doi: 10.1016/j.ins.2017.08.063. cited By 35.

D. Rey and M. Neuhäuser. Wilcoxon-signed-rank test. In *International encyclopedia of statistical science*, pages 1658–1659. Springer, 2011.

M. B. Rosson and J. M. Carroll. *Usability engineering: scenario-based development of human-computer interaction*. Morgan Kaufmann, 2002.

B. Sanz, C. Laorden, G. Alvarez, and P. G. Bringas. A threat model approach to attacks and countermeasures in on-line social networks. *In Proceedings of the 11th Reunion Espanola de Criptografıa y Seguridad de la Información (RECSI)*, pages 343–348, 2010.

R. Scandariato, K. Wuyts, and W. Joosen. A descriptive study of microsoft's threat modeling technique. *Requirements Engineering*, 20(2):163–180, 2015.

B. Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

Z. Shi, K. Graffi, D. Starobinski, and N. Matyunin. Threat modeling tools: A taxonomy. *IEEE Security & Privacy*, (01):2–13, 2021.

R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec. Protecting location privacy: optimal strategy against localization attacks. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 617–627, 2012.

A. Shostack. Experiences threat modeling at microsoft. *MODSEC@ MoDELS*, 2008: 35, 2008.

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

F. Shull, J. Carver, and G. H. Travassos. An empirical methodology for introducing software processes. *ACM SIGSOFT Software Engineering Notes*, 26(5):288–296, 2001.

M. Siddula, L. Li, and Y. Li. An empirical study on the privacy preservation of online social networks. *IEEE Access*, 6:19912–19922, 2018.

G. Sindre and A. L. Opdahl. Eliciting security requirements with misuse cases. *Requirements engineering*, 10(1):34–44, 2005.

O. Solon. Facebook says cambridge analytica may have gained 37m more users' data. *The Guardian*, 4, 2018.

J. Song, S. Lee, and J. Kim. Inference attack on browsing history of twitter users using public click analytics and twitter metadata. *IEEE Transactions on Dependable and Secure Computing*, 13(3):340–354, 2014.

X. Song, X. Wang, L. Nie, X. He, Z. Chen, and W. Liu. A personal privacy preserving framework: I let you know who can see what. pages 295–304, 2018. doi: 10.1145/3209978.3209995. cited By 3.

M. Sramka. Privacy scores: Assessing privacy risks beyond social networks. *Infocommunications Journal*, 4(4):36–41, 2012. cited By 1.

C. Tang, Y. Wang, H. Xiong, T. Yang, J. Hu, Q. Shen, and Z. Chen. Need for symmetry: Addressing privacy risks in online social networks. pages 534–541, 2011. doi: 10.1109/AINA.2011.57. cited By 4.

G. H. Travassos, D. Gurov, and E. Amaral. Introdução à engenharia de software experimental. 2002.

R. Tucker, C. Tucker, and J. Zheng. Privacy pal: Improving permission safety awareness of third party applications in online social networks. pages 1268–1273, 2015. doi: 10.1109/HPCC-CSS-ICESS.2015.83. cited By 2.

T. UcedaVelez and M. M. Morana. *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons, 2015.

H. Vu, R. Law, and G. Li. Breach of traveller privacy in location-based social media. *Current Issues in Tourism*, 22(15):1825–1840, 2019. doi: 10.1080/13683500.2018.1553151. cited By 2.

Y. Wang and R. Nepali. Privacy threat modeling framework for online social networks. pages 358–363, 2015. doi: 10.1109/CTS.2015.7210449. cited By 5.

C. Watanabe, T. Amagasa, and L. Liu. Privacy risks and countermeasures in publishing and mining social network data. pages 55–66, 2011. doi: 10.4108/icst.collaboratecom.2011.247177. cited By 6.

G. Wen, H. Liu, J. Yan, and Z. Wu. A privacy analysis method to anonymous graph based on bayes rule in social networks. pages 469–472, 2018. doi: 10.1109/CIS2018.2018.00111. cited By 0.

R. J. Wieringa. *Design science methodology for information systems and software engineering*. Springer, 2014.

J. Williams. Social networking applications in health care: threats to the privacy and security of health information. In *Proceedings of the 2010 ICSE workshop on software engineering in health care*, pages 39–49, 2010.

C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén. *Experimentation in software engineering*. Springer Science & Business Media, 2012.

K. Wuyts, R. Scandariato, and W. Joosen. Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software*, 96:122–138, 2014.

K. Wuyts, D. Van Landuyt, A. Hovsepyan, and W. Joosen. Effective and efficient privacy threat modeling through domain refinements. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pages 1175–1178, 2018.

W. Xiong and R. Lagerström. Threat modeling–a systematic literature review. *Computers & security*, 84:53–69, 2019.

H. Xu, H.-H. Teo, and B. Tan. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *ICIS 2005 proceedings*, page 71, 2005.

M. B. Yassein, S. Aljawarneh, and Y. A. Wahsheh. Survey of online social networks threats and solutions. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 375–380. IEEE, 2019.

W. Youyou, M. Kosinski, and D. Stillwell. Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4):1036–1040, 2015.

Y. Zeng, Y. Sun, L. Xing, and V. Vokkarane. Trust-aware privacy evaluation in online social networks. pages 932–938, 2014. doi: 10.1109/ICC.2014.6883439. cited By 5.

Y. Zeng, Y. Sun, L. Xing, and V. Vokkarane. A study of online social network privacy via the tape framework. *IEEE Journal on Selected Topics in Signal Processing*, 9(7): 1270–1284, 2015. doi: 10.1109/JSTSP.2015.2427774. cited By 7.

A. Zhang, C. Gunter, X. Xie, J. Han, K.-C. Chang, and X. Wang. Privacy risk in anonymized heterogeneous information networks. pages 595–606, 2014. doi: 10.5441/002/edbt.2014.53. cited By 7.

X. Zhang, L. Zhang, and C. Gu. Security risk estimation of social network privacy issue. pages 81–85, 2017. doi: 10.1145/3163058.3163073. cited By 2.

E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web*, pages 531–540, 2009.

Apêndice A

Guia prático

Guia Prático da PTMOL

Guia Prático da PTMOL

Segurança vs Privacidade

Violação de Privacidade

Descoberta e divulgação direta ou indireta de informações privadas que estão disponíveis publicamente, com ou sem conhecimento prévio do usuário

Violação de Segurança

Acesso não autorizado a dados privados, protegidos por mecanismos de segurança.

Ameaça de Privacidade

Evento indesejável real ou potencial com a capacidade de causar divulgação, exposição ou uso indevido de dados privados do usuário.

Privacy Threat MOdeling Language - PTMOL

Linguagem para a modelagem de ameaças de privacidade orientada a redes sociais online

O que é a PTMOL?

A **PTMOL** é uma linguagem que permite mapear previamente cenários de ameaças relevantes de privacidade, suas consequências e como elas podem ser mitigadas.

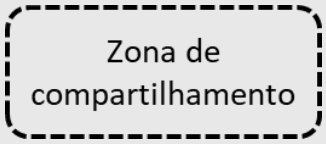
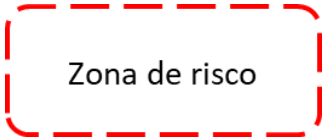
A **PTMOL** pode ser incorporada ao desenvolvimento de redes sociais online no estágio de design (projeto), visto que permite identificar previamente situações que possam comprometer a privacidade do usuário. Portanto, ajuda a expandir o entendimento sobre os ativos do usuário a serem protegidos, gerando várias melhorias em termos de redução de riscos.

Além disso, a **PTMOL** fornece um suporte estruturado para que designers não especialistas em privacidade raciocinem sobre cenários de ameaças relevantes.

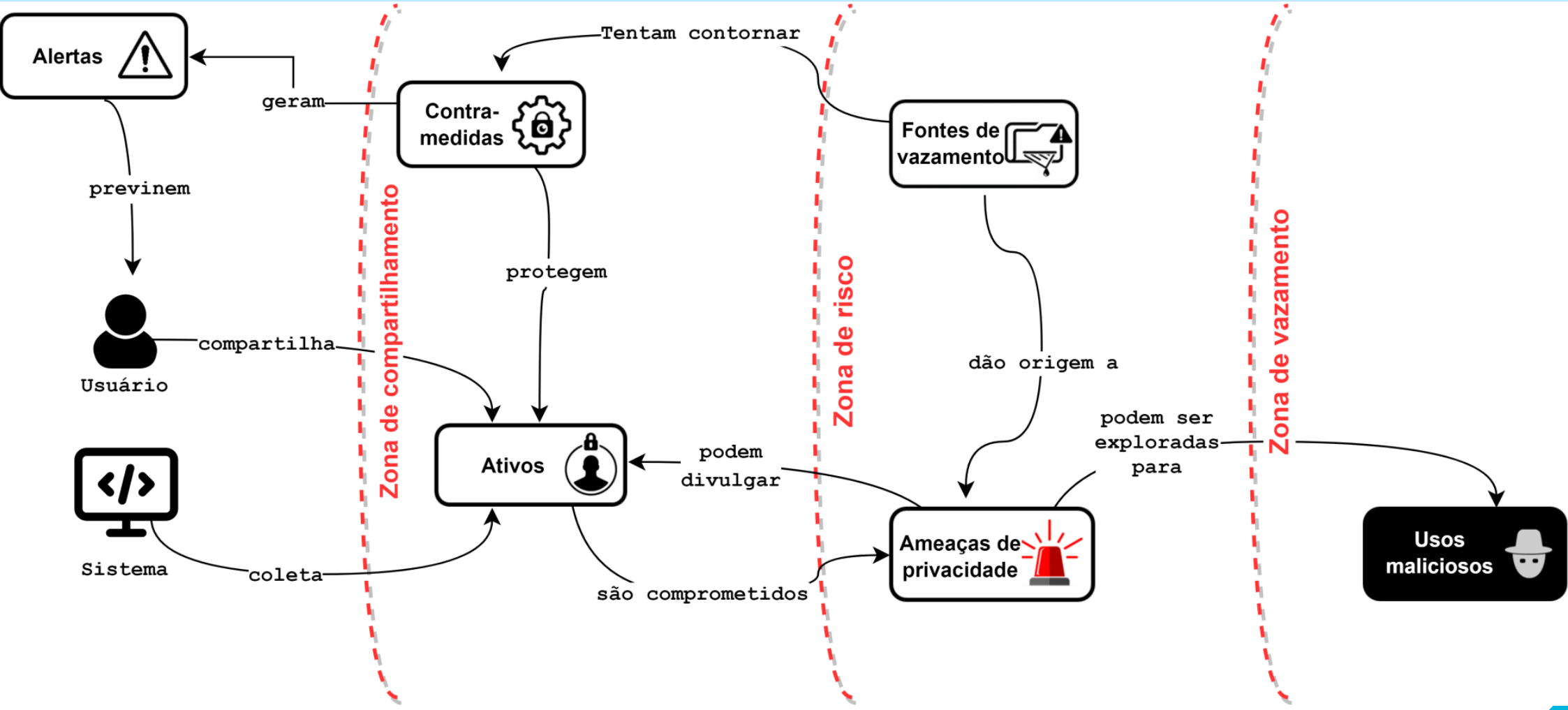
Notação da Linguagem PTMOL

Notação	Descrição
	Algo relacionado ao alvo (usuário) que possui um valor pessoal
	Uma situação indesejável que pode colocar em risco os ativos do usuário.
	Ação que um agente malicioso executa para violar a privacidade de um usuário.
	Agentes maliciosos que pode estar infiltrados dentro ou fora da rede para violar a privacidade do usuário.

Notação da Linguagem PTMOL

Notação	Descrição
	Representa um alerta do sistema para informar os usuários sobre qualquer ação com consequências importantes.
	Estratégia para mitigar ameaças de privacidade exploradas por agentes maliciosos
	Representa a zona de compartilhamento de ativos
	Representa a zona de risco referente as ameaças e ações do atacante
	Representa a zona de proteção referente aos alertas de prevenção e contramedidas

Privacy Threat MOdeling Language - PTMOL



Base de conhecimento da PTMOL

A base de conhecimento da PTMOL apoia o conhecimento em ameaças de privacidade através dos seguintes suportes:

Um ***template* de modelagem** que serve como apoio para uma representação estruturada de todas as informações que afetam a privacidade do usuário.

Um **catálogo de ameaças** que ajuda o designer a refletir sobre quais cenários de ameaça um usuário está potencialmente exposto e ações que um potencial atacante realizaria para explorar as ameaças e colocar em risco os ativos do usuário.

Uma **taxonomia de contramedidas** para auxiliar na formulação de estratégias preventivas para o tratamento das ameaças identificadas.

Processo de Aplicação da PTMOL

A PTMOL permite que o designer represente e, consequentemente, elabore e refine seu projeto em camadas, ou seja, aos poucos. Inicialmente, o designer (elemento a) deve compreender o domínio da RSO que deseja modelar. É necessária uma descrição dos recursos que permitem o usuário compartilhar informações no sistema ou de um eventual cenário de interação, onde o usuário compartilhará ativos no sistema.

a) Entendendo o cenário de ameaças	
b) *Template* de modelagem	
c) Modelo de ameaças	

Processo de Aplicação da PTMOL

Após entender um possível cenário de ameaças ao qual o usuário poderá está exposto, a PTMOL possibilita que o designer defina trechos da sua modelagem de ameaças a partir de padrões, ou *templates* integrados à linguagem, de modo que sua compreensão sobre o problema e possíveis soluções se amplie. O *template* de modelagem (elemento b) serve como apoio para uma representação estruturada de todas as informações que afetam a privacidade do usuário. Além disso, o *template* permite documentar todas as descobertas e ações do atacante, para que futuras alterações nas configurações do sistema, no cenário de ameaças e no ambiente de interação possam ser resolvidas rapidamente.

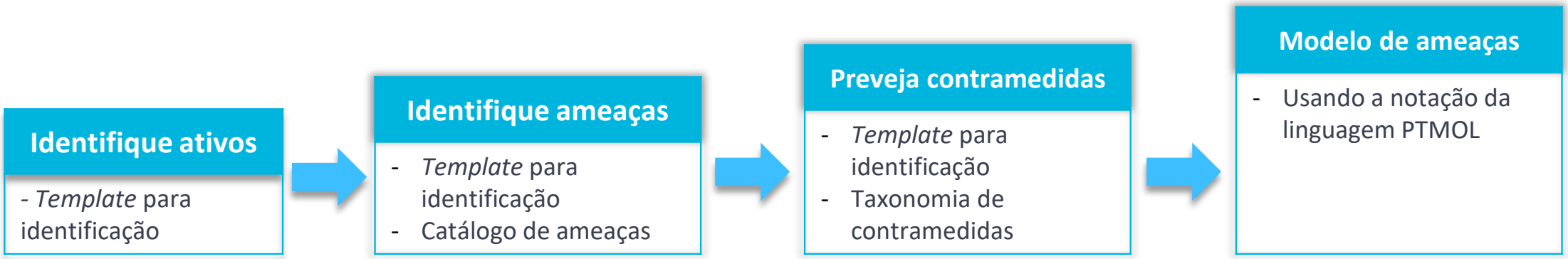
a) Entendendo o cenário de ameaças	
b) *Template* de modelagem	
c) Modelo de ameaças	

Processo de Aplicação da PTMOL

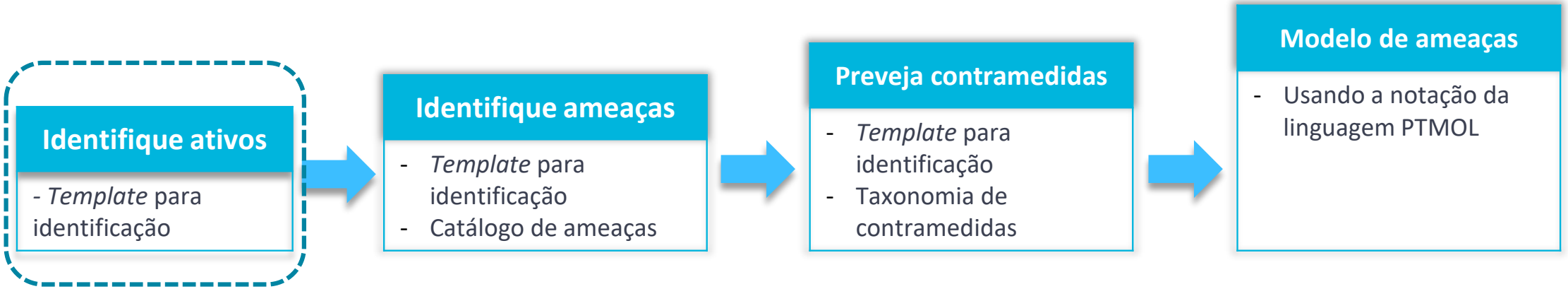
Após a análise de todas as informações identificadas anteriormente, o designer deverá produzir o modelo de ameaças (elemento c) resultante do projeto.

a) Entendendo o cenário de ameaças	
b) *Template* de modelagem	
c) Modelo de ameaças	

Etapas da modelagem com a PTMOL

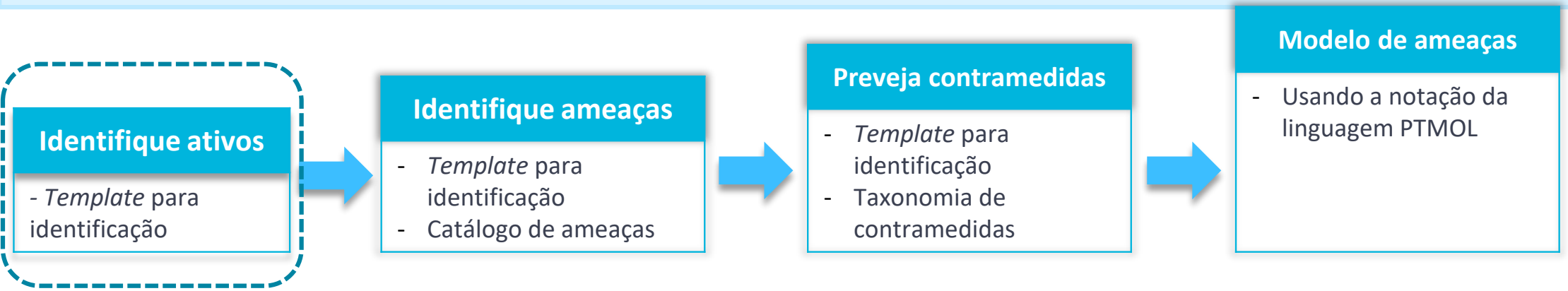


Identificando ativos



Nesta etapa, você deverá identificar os ativos a serem protegidos. Um ativo é algo relacionado ao alvo (usuário) que possui um valor pessoal. Você precisa compreender o que deve ser protegido, antes de começar a descobrir quais ameaças podem ocorrer. É essencial que você, como designer, tenha um entendimento sobre os ativos, pois as próximas etapas da modelagem serão direcionadas a eles. Existem dois tipos de ativos – aqueles compartilhados pelo usuário e aqueles coletados pelo sistema.

Identificando ativos



Ativos compartilhados pelo usuário

Dependendo da forma como o ativo foi compartilhado pelo usuário, diferentes ameaças podem ocorrer. Nesta visão, três formas de compartilhamento, e suas respectivas variantes, foram definidas. O ativo poderá ser compartilhado por meio de:

- Dados textuais: arquivos ou texto livre;
- Dados multimídia: fotos, áudios ou vídeos;
- Dados geográficos: geolocalização

Ativos coletados pelo sistema

Os ativos coletados pelo sistema são aquelas informações pessoais que não são compartilhadas pelos os usuários, mas que o sistema coleta e armazena em seus servidores. Essas informações podem estar associadas a duas categorias:

- Dados de relacionamento
- Dados de uso

Ativos compartilhados pelo usuário

O *template* de classificação de ativos permite que o designer liste todos os ativos extraídos do cenário de ameaças e classifique a sua forma de compartilhamento. Dependendo de como ativo foi compartilhamento na RSO, diferentes ameaças podem surgir. Por exemplo, a localização descrita de forma textual é diferente da localização compartilhada em tempo real (geolocalização).

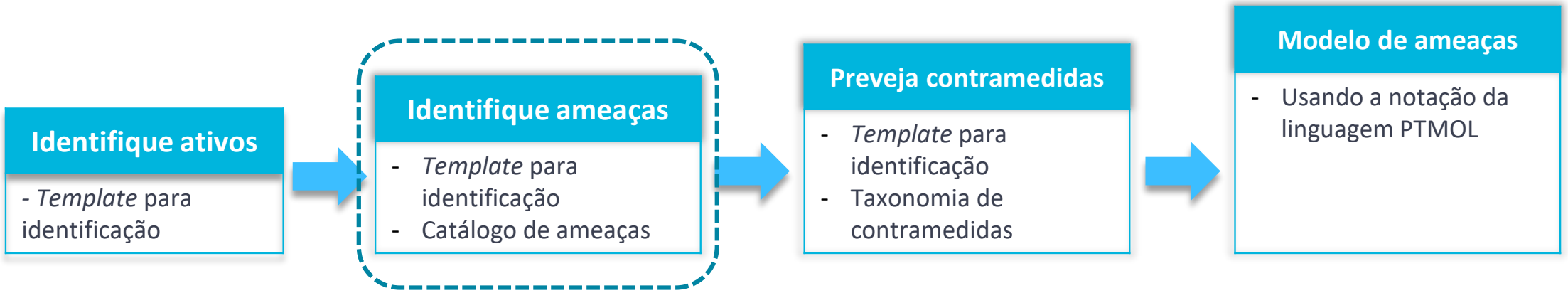
Ativos 	ATIVOS COMPARTILHADOS PELO USUÁRIO					
	Dado Textual		Dado multimídia			Dado geográfico
	Arquivo (PDF, DOC)	Texto livre	Foto	Vídeo	Áudio	Geolocalização
Ativo 1						
Ativo 2						
Ativo 3						
...						
Ativo n						
<Listar todos os ativos>	<Marcar com "X" a forma de compartilhamento do ativo>					

Ativos coletados pelo sistema

O outro *template* de classificação de ativos permite que o designer liste também todos os ativos coletados pelo sistema. Essas informações podem estar associadas a duas categorias, como dados de relacionamento e dados de uso.

Ativos 	ATIVOS COLETADOS PELO SISTEMA	
	Dados de uso 	Dados de relacionamento 
Ativo 1		
Ativo 2		
Ativo 3		
...		
Ativo n		
<Listar todos os ativos>	<Marcar com "X" se o ativo pertencer a essa categoria>	<Marcar com "X" se o ativo pertencer a essa categoria>

Identificando ameaças, fontes de vazamento e usos maliciosos

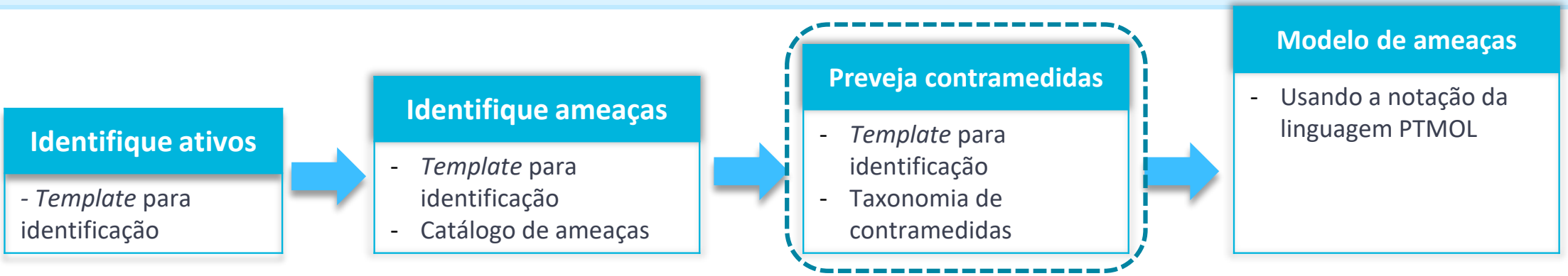


A segunda etapa pode ser considerada como uma das principais na execução do processo de modelagem de ameaças com a PTMOL. Neste etapa, você deve consultar o catálogo de ameaças integrada à linguagem e identificar quais delas podem ocorrer em relação ao ativo em análise. Para cada ativo listado, deve-se apontar uma ou mais ameaças de privacidade. Essa associação da ameaça ao ativo ajudará você a refletir sobre as possíveis fontes de vazamentos e os usos maliciosos previstos para executar a ameaça.

Identificando ameaças, fontes de vazamento e usos maliciosos

Ativos 	Classificação do ativo	Ameaças de privacidade 	Fontes de vazamento 	Usos maliciosos 
O que deve ser protegido?	Ativo coletado ou compartilhado?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	Valor pré-definido	Valor pré-definido	Valor pré-definido	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Classificar ativo>	<Associar ameaça [do catálogo] ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>

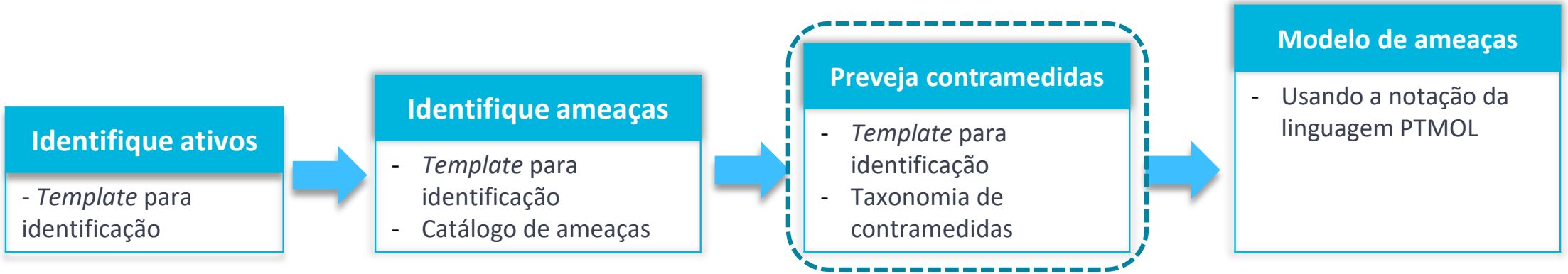
Prevendo contramedidas



Por fim, na última etapa, você terá que tomar decisões estratégicas que garantam uma maior assertividade na implantação de alertas e contramedidas adequadas para a proteção dos ativos. Após listar o conjunto de ameaças e suas consequências para a privacidade do usuário, o designer deve consultar a taxonomia implementada com propriedades de privacidade.

Propriedades de Privacidade	Definições
Desvinculação	Refere-se a capacidade de ocultar o link (relação) entre duas ou mais ações, identidades ou informações. O atacante não pode ser capaz de identificar se 2 itens estão relacionados.
Anonimato de Pseudonimato	O atacante não pode ser capaz de identificar um indivíduo dentro de um conjunto de indivíduos anônimos. Um pseudonimato é um identificador de um indivíduo diferente de um dos nomes reais dele.
Negação plausível	A negação plausível refere-se à capacidade de negar a realização de uma ação que outras partes não podem confirmar.
Confidencialidade	Refere-se a ocultação dos conteúdo dos dados ou liberação controlada desses conteúdos. No geral, a confidencialidade significa preservar as restrições de acesso e divulgação de informações.
Conscientização	Garantir que os usuários tenham conhecimento de seus dados pessoais e que apenas as informações mínimas necessárias sejam buscadas e utilizadas para permitir o desempenho da função a que se refere.
Transparência e conformidade	Exige que todo o sistema como controlador de dados informe o titular dos dados sobre a política de privacidade do sistema e permita que o titular dos dados especifique consentimentos em conformidade com a legislação, antes que os usuários acessem o sistema.
Não detecção	Refere-se a capacidade de ocultar as atividades do usuário.

Prevendo contramedidas

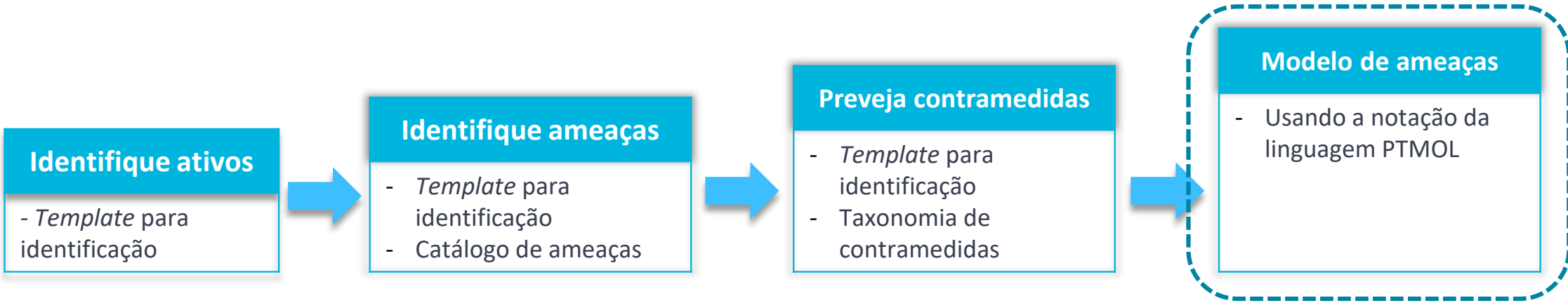


Para cada propriedade indicada como possivelmente violada, torna-se necessário transformá-la posteriormente em contramedida, de modo que esta possa reduzir ou dificultar os usos maliciosos previstos. Além disso, você também tem a opção de emitir alertas para informar os usuários sobre qualquer ação que pode causar violações graves para a sua privacidade. Com isso, você poderá pensar em contramedidas apropriadas para o sistema, permitindo a antecipação, ainda em fase de design, de decisões estratégicas para a proteção dos dados do usuário.

Prevendo contramedidas

Ativos 	Ameaças de privacidade 	Propriedade Violada	 Contramedidas	Alerta de prevenção 
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quais propriedades de privacidade foram violadas?	Qual estratégia adotar para mitigar as ameaças?	Que alerta poderia ser emitido para informar o usuário sobre consequências para a sua privacidade.
Ativo 1	Valor pré-definido	Valor pré-definido	Valor livre	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Listar todas as ameaças>	<Indicar a propriedade violada>	<Prever contramedidas>	<Gerar um alerta em situações graves>

Etapas da modelagem com a PTMOL



Apêndice B

Catálogo de ameaças da PTMOL

Cyberstalking 

Descrição geral

Uso da rede social para assediar ou perseguir um indivíduo, ou um grupo de indivíduos, com comportamento indesejado ou ameaçador, imposto repetidamente.

Os usuários revelam de forma frequente informações pessoais em seus perfis. Um agente malicioso pode coletar essas informações para usá-las indevidamente para cyberstalking

Impactos

- Reunir informações privadas do usuário para promover uma perseguição ou para assediar, ameaçar e induzir ao medo.
- Monitoramento e coleta obsessiva de informações privadas.
- Enviar links maliciosos para capturar dados privados.

Divulgação de Informações 

Descrição geral

Refere-se à descoberta e divulgação não autorizada de informações privadas. Essa divulgação pode expor diretamente uma enorme quantidade de dados pessoais do usuário, como endereço residencial, dados relacionados à saúde, dados de rotina e de relacionamento, dentre outros.

O compartilhamento dessas informações pessoais pode ter implicações negativas para a privacidade do usuário, como o uso indevido por parte de terceiros para fins diversos, como campanha política, marketing e anúncios indesejados.

Impactos

- Descoberta direta ou indireta de dados privados.
- Exposição não autorizada de dados pessoais.
- Divulgação de dados privados para campanha política, marketing e anúncios indesejados.

Ameaça à reputação 

Descrição geral

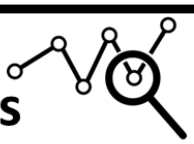
Devido às RSOs permitirem que indivíduos compartilhem diversas informações pessoais, seus usuários podem ser vítimas de danos à reputação.

Um agente malicioso ou uma entidade maliciosa pode obter acesso a informações íntimas e explorá-las para prejudicar a privacidade do usuário.

Além disso, os usuários podem se tornar vítimas de manipulação e distorção de dados. Atualmente, existem diversas ferramentas disponíveis para manipular e distorcer diversos dados.

Impactos

- Divulgar a intimidade do usuário para prejudicar a sua reputação.
- Coletar dados privados do usuário e usá-los para extorsão, discriminação ou constrangimento.
- Distorcer ou manipular indevidamente dados privados do usuário.

Inferência ou rastreamento de dados 

Descrição geral

É a coleta e combinação de dados para gerar ou descobrir informações pessoais do usuário que não estão diretamente compartilhadas em seus perfis nas RSOs, mas podem ser inferidas usando diferentes técnicas computacionais.

Os provedores da rede social rastreiam e analisam as atividades online do usuário (como navegação diária e preferências de compras, por exemplo) por meio de diversas técnicas de aprendizagem de máquina.

Como resultado, as redes sociais constroem perfis completos do usuário com o objetivo de vender produtos ou rastrear o seu comportamento. Tudo isso feito sem o conhecimento do usuário.

Impactos

- Rastreamento do comportamento do usuário.
- Criação de um perfil completo sobre a rotina do usuário.
- Inferência de dados para terceiros.
- Coleta e combinação de dados do usuário para prever outras informações não disponíveis publicamente.

Clonagem de perfil 

Descrição geral

Um agente malicioso pode utilizar os dados compartilhados por um determinado usuário e clonar o seu perfil, sem que a RSO ou aprópria vítima percebam a clonagem.

O agente malicioso cria uma identidade falsa para fazer os amigos da vítima acreditarem no novo perfil (falso). Com esse perfil criado, o agente malicioso poderá entrar em contato com a lista de amigos da vítima e enviar links para capturar dados privados.

Impactos

- Forjar atributos privados de um perfil real.
- Forjar a lista de contatos da vítima para que outros usuários acreditem no perfil clonado.
- Clonar um perfil em outra RSO na qual o usuário (vítima) ainda não está registrado.
- Fazer upload de fotos e vídeos inadequados no perfil clonado

Roubo de identidade 

Descrição geral

É um tipo de ameaça em que um agente malicioso obtém acesso ilegal a conta do usuário da RSO para capturar dados privados.

Diferentes técnicas maliciosas podem ser aplicadas por um atacante para realizar um roubo de identidade.

Por exemplo, um atacante pode enviar links para obter informações confidenciais, como senhas e códigos de autenticação. De posse desses dados, poderá obter acesso a conta do usuário na RSO e todo seu registro de atividades e dados pessoais.

Impactos

- Acesso indevido a dados confidenciais.
- Envio de informação privada para terceiros.
- Transferência de dados privados para uso malicioso.

Reconhecimento Facial 

Descrição geral

A maioria das RSOs permitem o compartilhamento de fotos. Os algoritmos de reconhecimento facial são capazes de identificar ou verificar uma pessoa a partir de uma imagem ou de uma fonte de vídeo.

Identificar o rosto de uma pessoa em uma foto ou vídeo e fazer referência cruzada com outros dados pode ser usado para expor informações pessoais do usuário.

Algoritmos combinados com outras tecnologias permitem encontrar usuários com uma boa precisão, sem o seu consentimento

Impactos

- Encontrar ou reconhecer usuários sem o seu consentimento.
- Cruzamento de imagens pessoais do usuário com outros dados privados.
- Coletar imagens para um banco de dados de biometria facial.
- Coletar reações faciais

Espionagem 

Descrição geral

É um tipo de monitoramento que permite, em tempo real, a coleta e o processamento de diversas atividades do usuário de RSOs, espionando principalmente suas atividades de perfil e relacionamentos com outros indivíduos.

Essa espionagem é uma ameaça social em que as atividades são frequentemente monitoradas nesses sistemas.

Uma das principais preocupações surge quando essa ameaça é explorada pelo governo, podendo realizar o monitoramento de cidadãos ou de adversários, visando atacá-los.

Impactos

- Monitorar as atividades de consumo do usuário para fins de anúncios personalizados.
- Distribuir informações monitoradas a terceiros.
- Monitoramento secreto do comportamento do usuário.

Gravação não autorizada

Descrição geral

Atualmente, muitas RSOs fornecem serviços de chat e videochamadas, proporcionando mais interação entre seus usuários. No entanto, muitas informações pessoais podem ser divulgadas ou coletadas via videochamada.

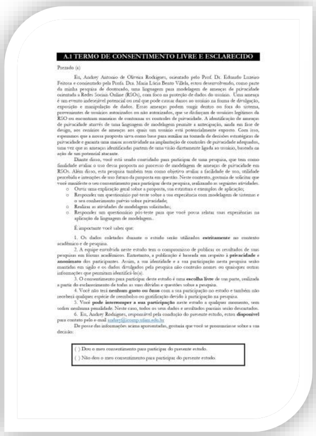
Um dos participantes pode facilmente realizar uma gravação não autorizada para posteriormente chantagear o outro participante (vítima). Além disso, um participante pode distorcer os dados da chamada e exibi-los inadequadamente.

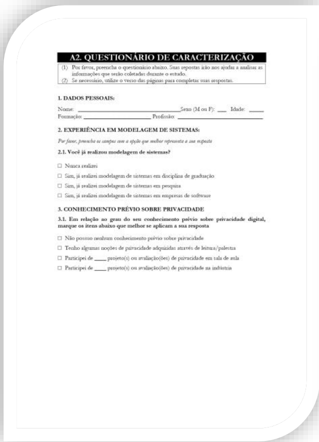
Impactos

- Gravar momentos íntimos e divulgar sem o consentimento do usuário.
- Distorcer dados da vídeo chamada e exibir de forma indevida.
- Acesso de pessoas desconhecidas a videochamada.

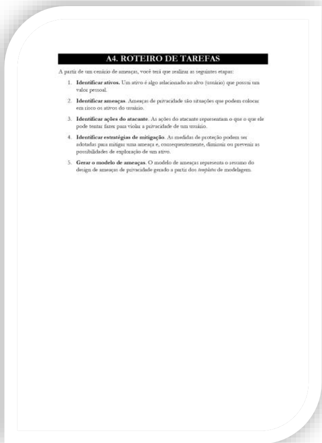
Apêndice C

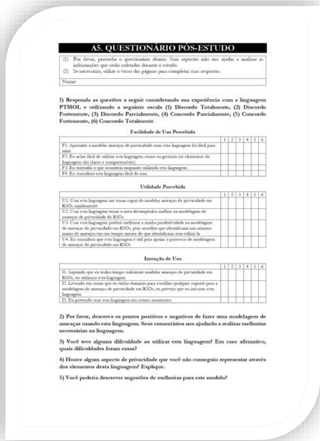
Materiais utilizados no primeiro, segundo e terceiro estudo


A.1 TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO


A2. QUESTIONÁRIO DE CARACTERIZAÇÃO


A3. CENÁRIO DO ESTUDO PRELIMINAR


A4. ROTEIRO DE TAREFAS


A5. QUESTIONÁRIO PÓS-ESTUDO

A.1 TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Prezado (a)

Eu, Andrey Antonio de Oliveira Rodrigues, orientado pelo Prof. Dr. Eduardo Luzeiro Feitosa e coorientado pela Profa. Dra. Maria Lúcia Bento Villela, estou desenvolvendo, como parte da minha pesquisa de doutorado, uma linguagem para modelagem de ameaças de privacidade orientada a Redes Sociais Online (RSOs), com foco na proteção de dados do usuário. Uma ameaça é um evento indesejável potencial ou real que pode causar danos ao usuário na forma de divulgação, exposição e manipulação de dados. Essas ameaças podem surgir dentro ou fora do sistema, provenientes de usuários autorizados ou não autorizados, que se disfarçam de usuários legítimos da RSO ou encontram maneiras de contornar os controles de privacidade. A identificação de ameaças de privacidade através de uma linguagem de modelagem permite a antecipação, ainda em fase de design, aos cenários de ameaças aos quais um usuário está potencialmente exposto. Com isso, esperamos que a nossa proposta sirva como base para auxiliar na tomada de decisões estratégicas de privacidade e garanta uma maior assertividade na implantação de controles de privacidade adequados, uma vez que as ameaças identificadas partem de uma visão diretamente ligada ao usuário, baseada na ação de um potencial atacante.

Diante disso, você está sendo convidado para participar de uma pesquisa, que tem como finalidade avaliar o uso dessa proposta no processo de modelagem de ameaças de privacidade em RSOs. Além disso, esta pesquisa também tem como objetivo avaliar a facilidade de uso, utilidade percebida e intenções de uso futuro da proposta em questão. Neste contexto, gostaria de solicitar que você manifeste o seu consentimento para participar desta pesquisa, realizando as seguintes atividades.

- Ouvir uma explicação geral sobre a proposta, sua estrutura e exemplos de aplicação;
- Responder um questionário pré-teste sobre a sua experiência com modelagem de sistemas e o seu conhecimento prévio sobre privacidade;
- Realizar as atividades de modelagem solicitadas;
- Responder um questionário pós-teste para que você possa relatar suas experiências na aplicação da linguagem de modelagem..

É importante você saber que:

1. Os dados coletados durante o estudo serão utilizados **estritamente** no contexto acadêmico e de pesquisa.
2. A equipe envolvida neste estudo tem o compromisso de publicar os resultados de suas pesquisas em fóruns acadêmicos. Entretanto, a publicação é baseada em respeito à **privacidade** e **anonimato** dos participantes. Assim, a sua identidade e a sua participação nesta pesquisa serão mantidas em sigilo e os dados divulgados pela pesquisa não conterão nomes ou quaisquer outras informações que permitam identificá-lo(a).
3. O consentimento para participar deste estudo é uma **escolha livre** de sua parte, realizada a partir do esclarecimento de todas as suas dúvidas e questões sobre a pesquisa.
4. Você não terá **nenhum gasto ou ônus** com a sua participação no estudo e também não receberá qualquer espécie de reembolso ou gratificação devido à participação na pesquisa.
5. Você **pode interromper a sua participação** neste estudo a qualquer momento, sem sofrer nenhuma penalidade. Neste caso, todos os seus dados e resultados parciais serão descartados.
6. Eu, Andrey Rodrigues, responsável pela condução do presente estudo, estou **disponível** para contato pelo e-mail andrey@icomp.ufam.edu.br

De posse das informações acima apresentadas, gostaria que você se pronunciasse sobre a sua decisão:

( ) Dou o meu consentimento para participar do presente estudo.

( ) Não dou o meu consentimento para participar do presente estudo.

QUESTIONÁRIO DE CARACTERIZAÇÃO DO 1º E 2º ESTUDO

(1) Por favor, preencha o questionário abaixo. Suas repostas irão nos ajudar a analisar as informações que serão coletadas durante o estudo.
(2) Se necessário, utilize o verso das páginas para completar suas respostas.

1. DADOS PESSOAIS:

Nome: _____Sexo (M ou F): ___ Idade: _____
Formação: _____ Profissão: _____

2. EXPERIÊNCIA EM MODELAGEM DE SISTEMAS:

Por favor, preencha os campos com a opção que melhor representa a sua resposta

2.1. Você já realizou modelagem de sistemas?

☐ Nunca realizei

☐ Sim, já realizei modelagem de sistemas em disciplina de graduação

☐ Sim, já realizei modelagem de sistemas em pesquisa

☐ Sim, já realizei modelagem de sistemas em empresas de software

3. CONHECIMENTO PRÉVIO SOBRE PRIVACIDADE

3.1. Em relação ao grau do seu conhecimento prévio sobre privacidade digital, marque os itens abaixo que melhor se aplicam a sua resposta

☐ Não possuo nenhum conhecimento prévio sobre privacidade

☐ Tenho algumas noções de privacidade adquiridas através de leitura/palestra

☐ Participei de ____ projeto(s) ou avaliação(ões) de privacidade em sala de aula

☐ Participei de ____ projeto(s) ou avaliação(ões) de privacidade na indústria

CENÁRIO DO PRIMEIRO ESTUDO

Instruções:
Por favor, execute a modelagem de ameaças de privacidade usando a PTMOL, com base no cenário. Em seguida, gere o modelo de ameaças usando a ferramenta *Drawio*. Após finalizar o modelo, salve, exporte em PNG e envie para o e-mail: andrey@icomp.ufam.edu.br

Cenário de Ameaça:

Ao se cadastrar na rede social, Maria, usuária novata, procura perfis que ofereçam serviços de reparos residenciais com atendimento rápido e fácil. Maria encontra um perfil e resolve mandar uma mensagem via chat para saber mais informações sobre os serviços prestados. No entanto. Maria não sabe que esse perfil trata-se de uma página gerenciada por um agente malicioso – João. Ao receber a mensagem, João inicia a conversa com Maria que informa qual serviço deseja contratar. Inicialmente, João pergunta se Maria não gostaria de fazer um orçamento sobre o serviço e lhe envia uma mensagem solicitando alguns dados: nome completo, número de telefone e e-mail para contato. Maria prontamente envia os dados solicitados e aguarda o orçamento. No outro dia, João informa que o orçamento de Maria está em andamento e que precisa ver algumas fotos da sua casa para saber o estado do ambiente no qual Maria solicitou o reparo. Maria envia fotos e vídeos mostrando partes da sua residência as quais necessitam de reparos. Ao receber as imagens, João informa que ainda não consegue criar um orçamento somente com aquelas imagens e vídeos enviados e solicita uma visita técnica. Maria responde a mensagem perguntando se João gostaria que ela enviasse o seu endereço. João prontamente afirma que quer o seu endereço e também a sua localização para ter uma rota mais precisa. Maria envia o seu endereço e sua localização.

CENÁRIO DO SEGUNDO ESTUDO

Instruções:
Por favor, execute a modelagem de ameaças de privacidade usando a PTMOL, com base no cenário. Em seguida, gere o modelo de ameaças usando o *template* fornecido.

Cenário de Ameaça:

Cristiana resolve criar uma conta em uma rede social online com propósito de interagir mais com seus amigos. Ao criar a conta, Cristina fornece alguns dados pessoais, como: nome completo, nome de perfil, e-mail e uma pequena biografia pessoal, todos esses dados ficarão disponíveis publicamente. Após informar esses dados, Cristina insere uma foto em seu perfil. Como primeira postagem, Cristina publica um vídeo com a seguinte legenda "Arrumando as malas para uma viagem". Nesse vídeo, Cristina também insere a sua localização atual. Cristina observa que existe um filtro na rede social e ele é pago. Cristina resolve comprar um filtro e fornece algumas informações de pagamento, como o número do cartão de crédito e outras informações sobre o cartão, como detalhes de cobrança, entrega e contato.

CENÁRIO DO TERCEIRO ESTUDO

Documento que descreve como a rede social pretende tratar o compartilhamento, coleta e processamento de dados do usuário.

I. Quais tipos de informações pretendemos coletar?

A Rede Social Online pretende tratar diversas informações sobre o usuário. Os tipos de informações que serão coletadas dependem de como o usuário utiliza o sistema.

Algo que o usuário e outras pessoas pretendem fazem ou fornecer.

- **Informações e conteúdo que o usuário fornece**. Pretendemos coletar o conteúdo das postagens e outras informações que usuário pretende fornecer ao utilizar nossa rede social, inclusive quando o usuário for se cadastrar para criar uma conta, criar ou compartilhar um conteúdo, enviar mensagens ou se comunicar com outras pessoas. Isso pode incluir nome, nome de usuário, e- mail, foto de perfil, localização, documentos, entre outros. Nossos sistemas também pretendem processar automaticamente o conteúdo que o usuário e outras pessoas queiram fornecer a fim de analisar o contexto incluído nesses itens para as finalidades descritas abaixo.
    - **Dados com proteções especiais**: é possível o usuário optar por fornecer informações nos campos de perfil sobre a sua opção religiosa, preferência política ou saúde. Essas e outras informações (como origem racial ou étnica, crenças filosóficas ou filiações sindicais) podem estar sujeitas a proteções especiais de acordo com as leis de proteção do país do usuário.
- **Redes e conexões**. Pretendemos coletar informações sobre as pessoas, as contas e os grupos com os quais o usuário se conecta e sobre como ele interage com a nossa rede social. Também pretendemos coletar informações de contato caso o usuário as carregue, sincronize ou importe de um dispositivo (como uma agenda de contatos, um registro de chamadas ou um histórico de SMS).
- **Seu uso**. Pretendemos coletar informações sobre como o usuário utiliza nossa rede social, como o tipo de conteúdo que o usuário visualiza ou com o qual se envolve; os recursos que o usuário utiliza; as ações que o usuário realiza; e o tempo, frequência e duração das suas atividades. Por exemplo, pretendemos registrar quando o usuário está utilizando e a última vez que usou nossa rede social e quais publicações, vídeos e outro conteúdo o usuário visualizou nos nossos sistemas. Nós também pretendemos coletar informações sobre como o usuário utiliza recursos com a nossa câmera.
- **Informações sobre transações realizadas na rede social.** Se o usuário for utilizar nossa rede social para compras ou outras transações financeiras (compra em um jogo ou realiza uma doação), nós pretendemos coletar informações sobre a compra ou transação. Isso inclui informações de pagamento, como o número do cartão de crédito ou débito e outras informações sobre o cartão do usuário, como detalhes de cobrança, entrega e contato.

ROTEIRO DE TAREFAS DO PRIMEIRO ESTUDO

A partir do cenário de ameaças, você terá que realizar as seguintes etapas:

1. **Identificar ativos.** Um ativo é algo relacionado ao alvo (usuário) que possui um valor pessoal.
2. **Identificar ameaças**. Ameaças de privacidade são situações que podem colocar em risco os ativos do usuário.
3. **Identificar ações do atacante**. As ações do atacante representam o que o que ele pode tentar fazer para violar a privacidade de um usuário.
4. **Identificar estratégias de mitigação**. As medidas de proteção podem ser adotadas para mitigar uma ameaça e, consequentemente, diminuir ou prevenir as possibilidades de exploração de um ativo.

Apêndice D

Materiais utilizados no estudo com especialistas

INSTRUÇÕES PARA O ESTUDO COM ESPECIALISTAS

Olá, você está sendo convidado para participar de uma pesquisa que tem como principal finalidade avaliar o cenário de ameaças de privacidade que um usuário poderá estar potencialmente exposto ao compartilhar informações pessoais em uma Rede Social Online (RSO). É importante você saber que sua avaliação será realizada em uma rede social representada através de um diagrama de classes. Assim, sua avaliação será direcionada para um sistema que ainda está em nível de design (projeto).

Inicialmente, você deverá compreender o domínio da RSO que será avaliada. Para isso, consulte o diagrama de classes fornecido, que descreve todos os recursos que permitem o usuário compartilhar informações no sistema.

Após entender o domínio da aplicação, use o seu conhecimento para apontar possíveis cenários de ameaças ao qual o usuário poderá está exposto e todas as informações que podem afetar a sua privacidade. Para isso, registre as suas descobertas em um documento a parte, de modo que sua avaliação possa ser descrita de forma detalhada.

Durante a sua avaliação, você deverá identificar os seguintes pontos:

1 – Ativos a serem protegidos:

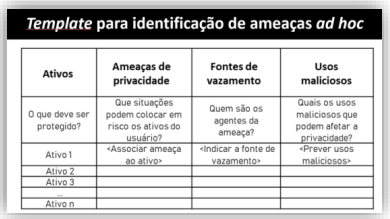
Um ativo é algo relacionado ao alvo (usuário) que possui um valor pessoal. Você precisa compreender o que deve ser protegido, antes de começar a descobrir quais ameaças podem ocorrer.

2 – Ameaças de Privacidade:

Nesta etapa, você deve indicar quais ameaças de privacidade podem ocorrer em relação aos ativos em análise. Para cada ativo listado, deve-se apontar uma ou mais ameaças de privacidade. Essa associação da ameaça ao ativo ajudará você a refletir sobre as possíveis fontes de vazamentos e os usos maliciosos.

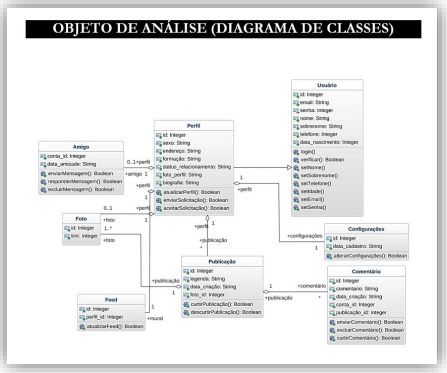
3 – Fontes de vazamento e usos maliciosos previstos:

Nesta etapa, você poderá indicar quais seriam as principais fontes de vazamento do sistema e também deverá indicar os principais usos maliciosos previstos, caso uma ameaça seja executada.



Template* para identificação de ameaças *ad hoc

Ativos	Ameaças de privacidade	Fontes de vazamento	Usos maliciosos
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	<Associar ameaça ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>
Ativo 2			
Ativo 3			
...			
Ativo n			



OBJETO DE ANÁLISE (DIAGRAMA DE CLASSES)

INSTRUÇÕES PARA O ESTUDO COM ESPECIALISTAS

Olá, você está sendo convidado para participar de uma pesquisa que tem como principal finalidade avaliar o cenário de ameaças de privacidade que um usuário poderá estar potencialmente exposto ao compartilhar informações pessoais em uma Rede Social Online (RSO). É importante você saber que sua avaliação será realizada em uma rede social representada através de um diagrama de classes. Assim, sua avaliação será direcionada para um sistema que ainda está em nível de design (projeto).

Inicialmente, você deverá compreender o domínio da RSO que será avaliada. Para isso, consulte o diagrama de classes fornecido, que descreve todos os recursos que permitem o usuário compartilhar informações no sistema.

Após entender o domínio da aplicação, use o seu conhecimento para apontar possíveis cenários de ameaças ao qual o usuário poderá está exposto e todas as informações que podem afetar a sua privacidade. Para isso, registre as suas descobertas em um documento a parte, de modo que sua avaliação possa ser descrita de forma detalhada.

Durante a sua avaliação, você deverá identificar os seguintes pontos:

1 – Ativos a serem protegidos:

Um ativo é algo relacionado ao alvo (usuário) que possui um valor pessoal. Você precisa compreender o que deve ser protegido, antes de começar a descobrir quais ameaças podem ocorrer.

2 – Ameaças de Privacidade:

Nesta etapa, você deve indicar quais ameaças de privacidade podem ocorrer em relação aos ativos em análise. Para cada ativo listado, deve-se apontar uma ou mais ameaças de privacidade. Essa associação da ameaça ao ativo ajudará você a refletir sobre as possíveis fontes de vazamentos e os usos maliciosos.

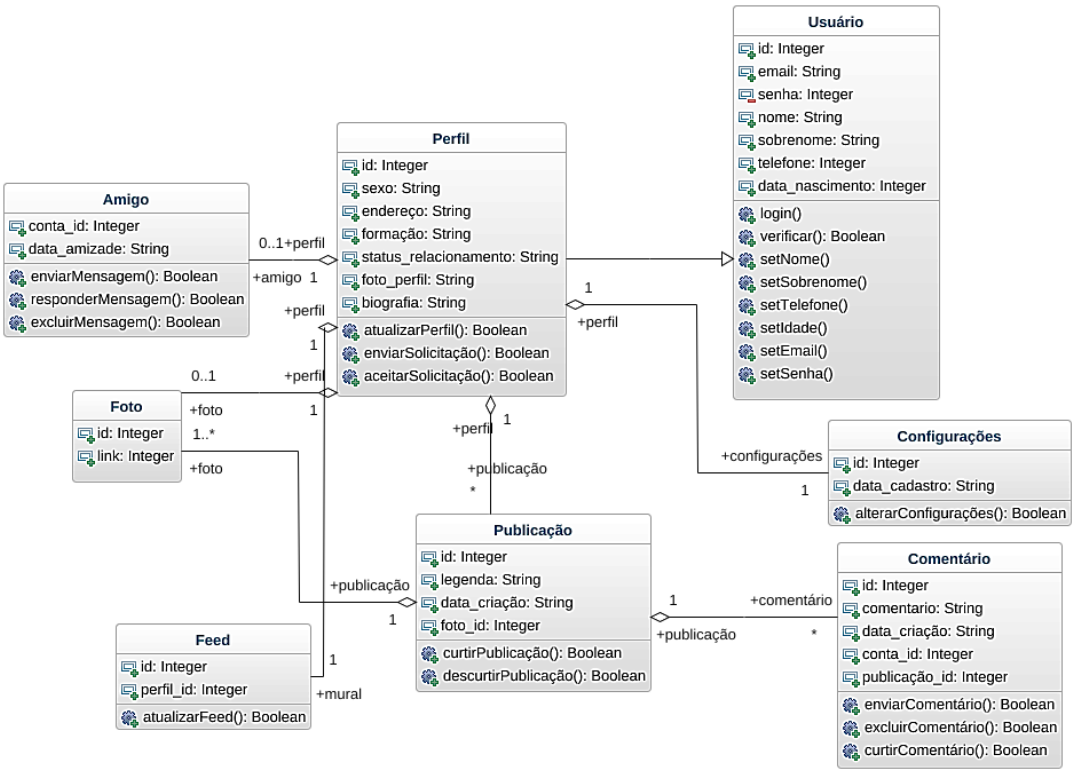
3 – Fontes de vazamento e usos maliciosos previstos:

Nesta etapa, você poderá indicar quais seriam as principais fontes de vazamento do sistema e também deverá indicar os principais usos maliciosos previstos, caso uma ameaça seja executada.

Template para identificação de ameaças *ad hoc*

Ativos	**Ameaças de privacidade**	**Fontes de vazamento**	**Usos maliciosos**
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	<Associar ameaça ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>
Ativo 2			
Ativo 3			
...			
Ativo n			

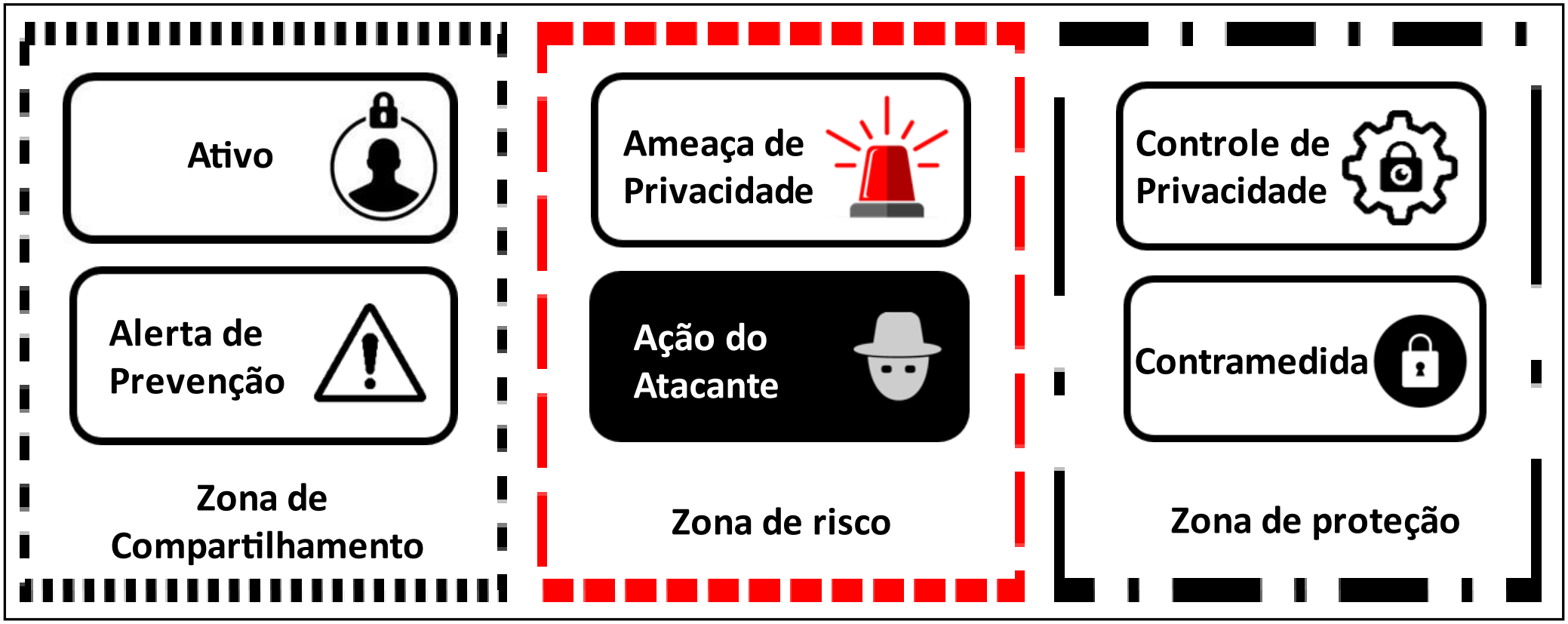
OBJETO DE ANÁLISE (DIAGRAMA DE CLASSES)



Apêndice E

Evolução da PTMOL

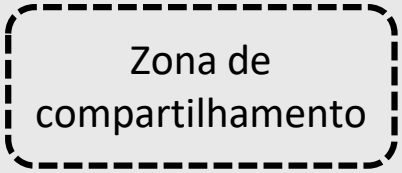
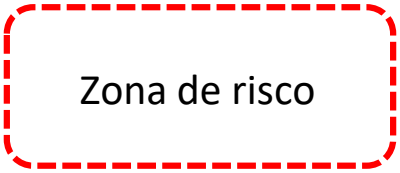
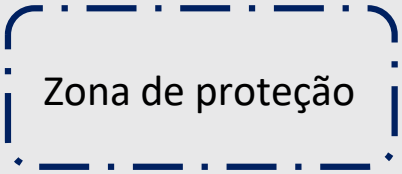
Versão 1 - Notação da Linguagem



Versão 1 - Notação da Linguagem

Notação	Descrição
Ativo 	Algo relacionado ao alvo (usuário) que possui um valor pessoal
Ameaça de Privacidade 	Uma situação indesejável que pode colocar em risco os ativos do usuário.
Ação do atacante 	Ação que o atacante executa para violar a privacidade de um usuário.
Alerta de Prevenção 	Representa um alerta do sistema para informar os usuários sobre qualquer ação com consequências importantes.
Contramedida 	Descreve a ação do sistema para mitigar ameaças de privacidade exploradas por atacantes

Versão 1 - Notação da Linguagem

Notação	Descrição
	Representa a zona de compartilhamento de ativos
	Representa a zona de risco referente as ameaças e ações do atacante
	Representa a zona de proteção referente aos alertas de prevenção e contramedidas

Versão 1 – *Template* para identificação de ativos

Ativo 	FORMA DE COMPARTILHAMENTO DO ATIVO					
	Dados textuais		Dados multimídia			Dados geográficos
	Arquivo (PDF, DOC)	Texto livre	Fotos	Vídeos	Áudios	Geolocalização

Versão 1 – *Template* para identificação de ameaças

Ativo 	FORMA DE COMPARTILHAMENTO	Ameaça de Privacidade 	Ação do atacante 
	Texto livre		
	Fotos		
	Vídeos		

Versão 1 – *Template* para identificação de contramedidas

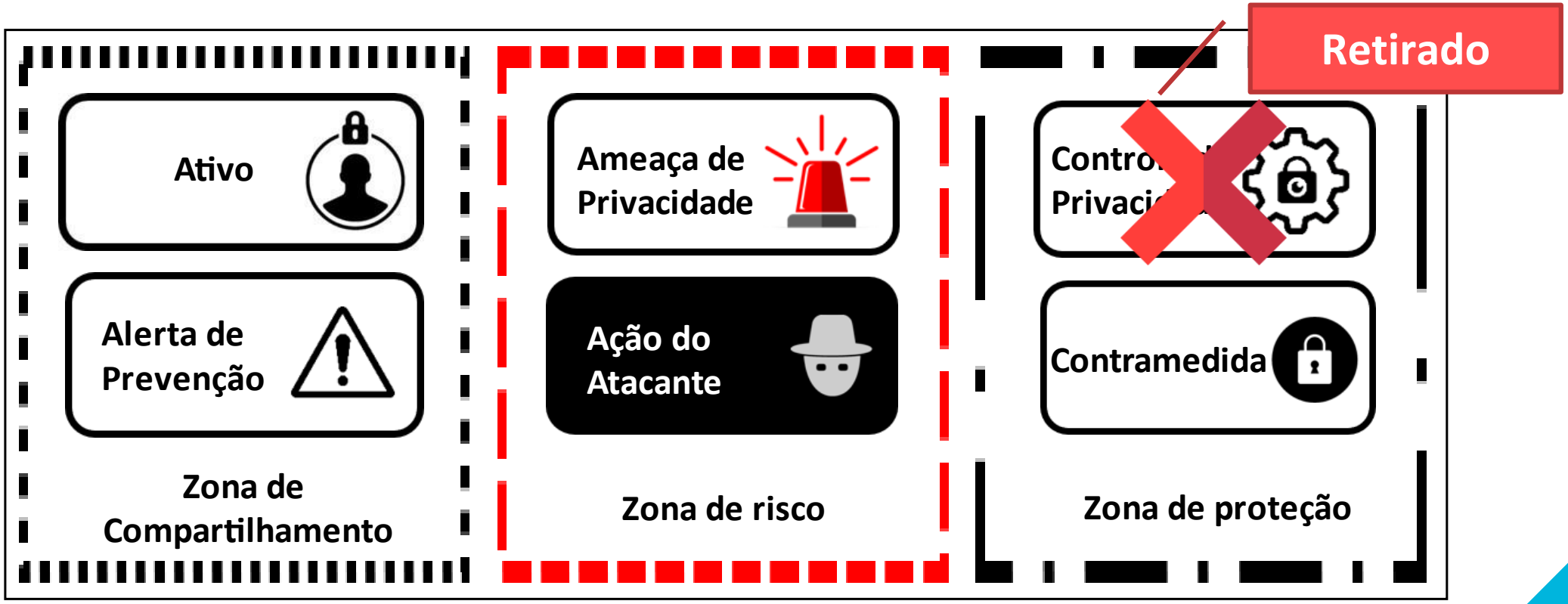
Ameaça de Privacidade 	Ação do atacante 	Alerta de Prevenção 

Versão 1 – *Template* para identificação de contramedidas

Ativo 	FORMA DE COMPARTILHAMENTO	Ameaça de Privacidade 	Contramedida 
	Texto livre		
	Fotos		
	Vídeos		

Versão 1 - Melhorias e Evolução

O **elemento "controle"** também é uma **forma de contramedida** para prevenir ou neutralizar uma ameaça. Portanto, a finalidade do elemento está fortemente ligada ao propósito da contramedida. Com isso, optou-se por **retirar o elemento "controle"** da composição de elementos da PTMOL e deixar somente os **elementos "alerta de prevenção" e "contramedidas" como estratégias de mitigação**.



Versão 1 - Melhorias e Evolução

O **elemento “ações do atacante”**, que permitia o designer criar um raciocínio sobre as possíveis ações que um agente malicioso pode realizar quando estiver de posse dos ativos do usuário, **foi renomeado**. Para deixar mais claro o propósito do componente da PTMOL, o nome do elemento foi alterado para **“usos maliciosos”**.

Versão 1 - Melhorias e Evolução

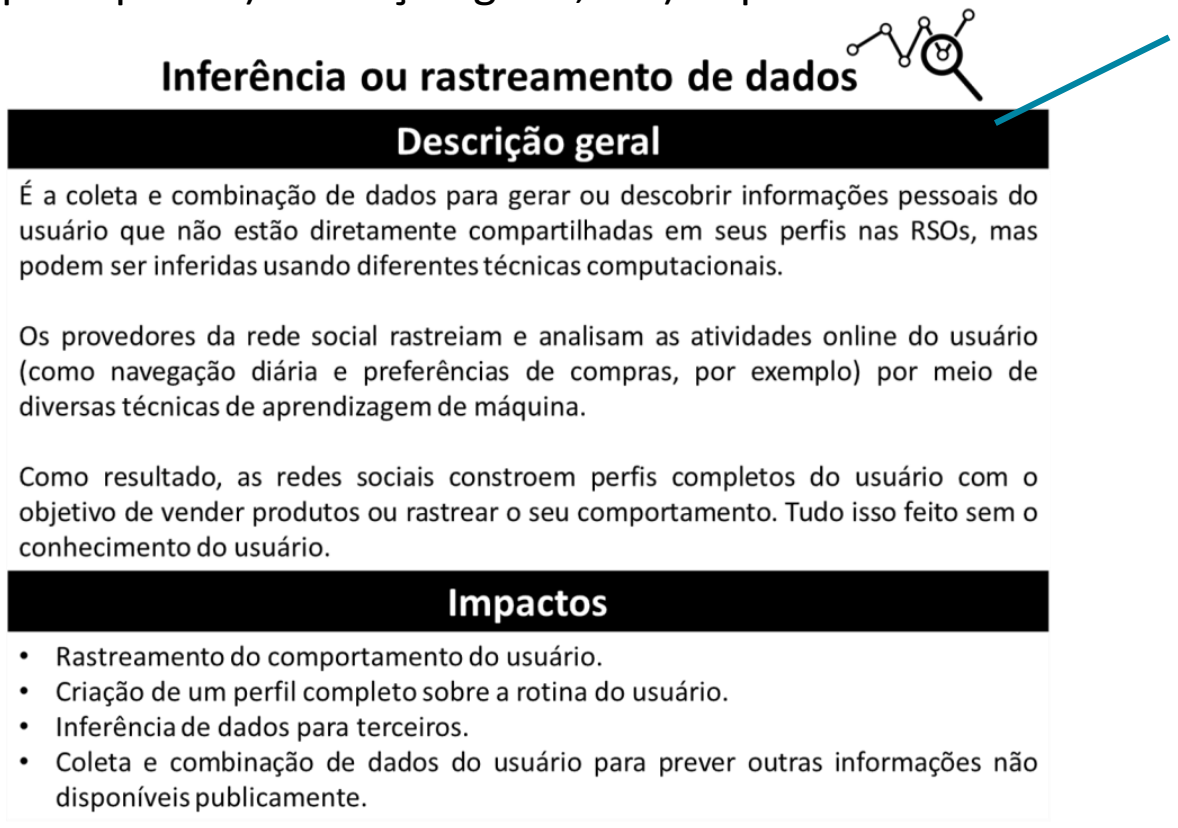
O *template* para classificação de ativos era destinado somente para listar ativos compartilhados pelo usuário no sistema. Tal *template* não previa a classificação dos ativos coletados e processados pelo sistema, que não necessariamente são compartilhados pelo usuário, mas que são coletados e combinados para gerar outras informações pessoais.

	ATIVOS COLETADOS PELO SISTEMA	
	CATEGORIAS	
	Dados de relacionamento	Dados de uso

Novo *template* para complementação da classificação de ativos

Versão 1 - Melhorias e Evolução

Criou-se uma descrição geral para cada tipo de ameaça da PTMOL pois, durante os estudos, percebeu-se que nem sempre os participantes estavam familiarizados com os conceitos generalistas de um tipo específico de ameaça. Um resumo de cada categoria de ameaça foi organizado levando em consideração dois itens principais: a) descrição geral; e b) impactos.



Inferência ou rastreamento de dados

Descrição geral

É a coleta e combinação de dados para gerar ou descobrir informações pessoais do usuário que não estão diretamente compartilhadas em seus perfis nas RSOs, mas podem ser inferidas usando diferentes técnicas computacionais.

Os provedores da rede social rastreiam e analisam as atividades online do usuário (como navegação diária e preferências de compras, por exemplo) por meio de diversas técnicas de aprendizagem de máquina.

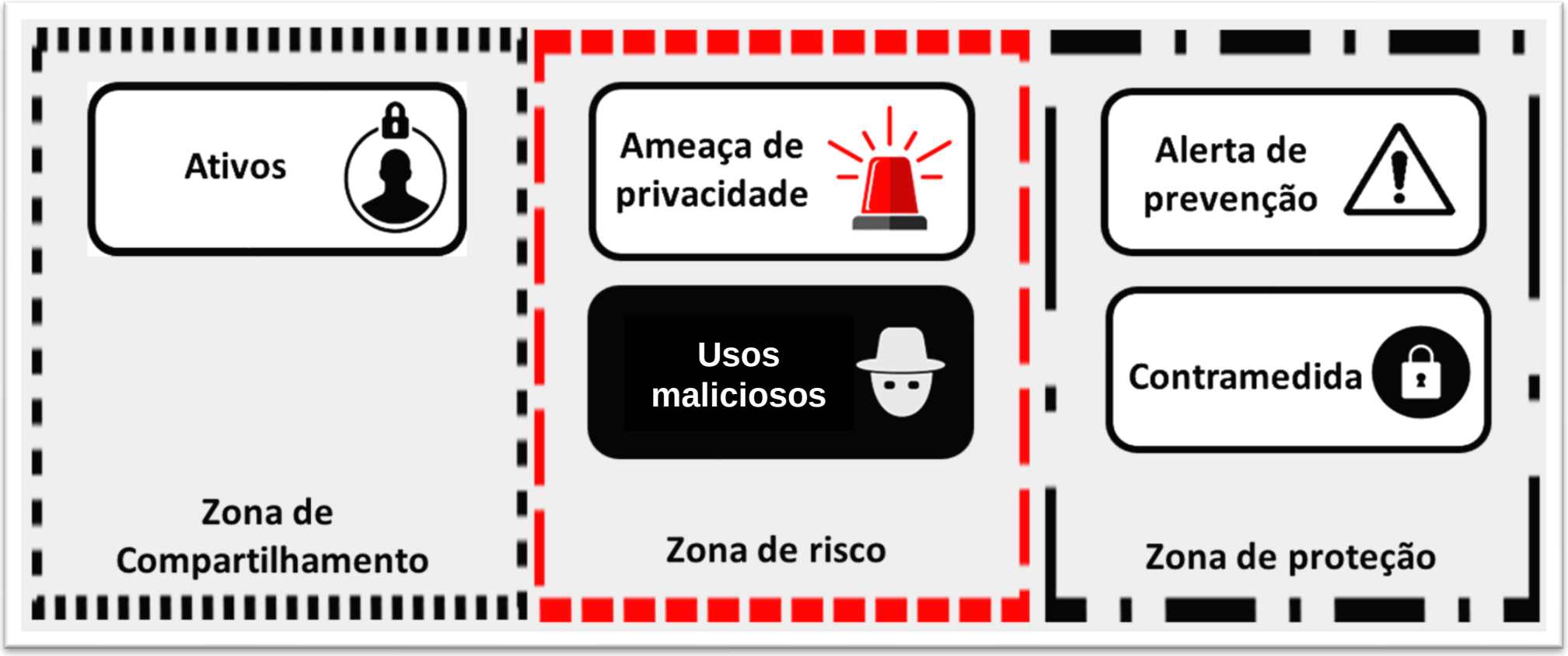
Como resultado, as redes sociais constroem perfis completos do usuário com o objetivo de vender produtos ou rastrear o seu comportamento. Tudo isso feito sem o conhecimento do usuário.

Impactos

- Rastreamento do comportamento do usuário.
- Criação de um perfil completo sobre a rotina do usuário.
- Inferência de dados para terceiros.
- Coleta e combinação de dados do usuário para prever outras informações não disponíveis publicamente.

Exemplo do refinamento no catálogo de ameaças

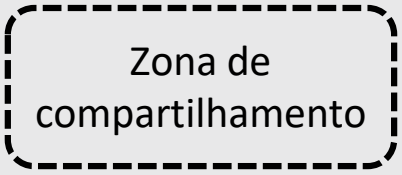
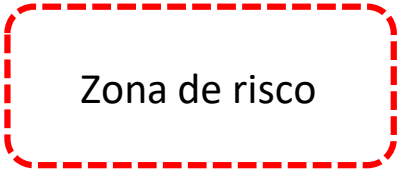
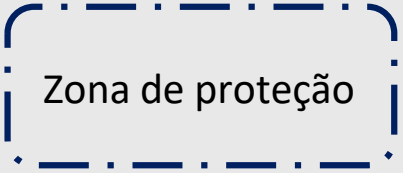
Versão 2 – Notação da Linguagem



Versão 2 – Notação da Linguagem

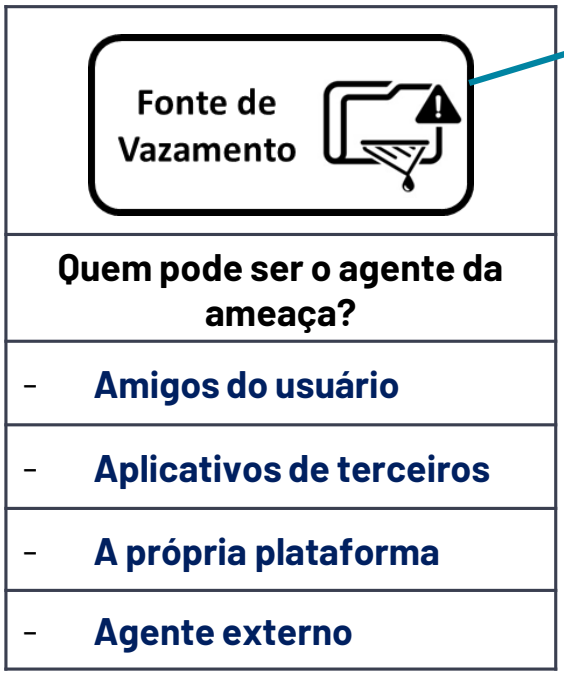
Notação	Descrição
Ativo 	Algo relacionado ao alvo (usuário) que possui um valor pessoal
Ameaça de Privacidade 	Uma situação indesejável que pode colocar em risco os ativos do usuário.
Usos maliciosos 	Prever qual comportamento indevido ou malicioso o atacante pode executar ao obter acesso aos dados privados do usuário
Alerta de Prevenção 	Representa um alerta do sistema para informar os usuários sobre qualquer ação com consequências importantes.
Contramedida 	Descreve a ação do sistema para mitigar ameaças de privacidade exploradas por atacantes

Versão 2 – Notação da Linguagem

Notação	Descrição
	Representa a zona de compartilhamento de ativos
	Representa a zona de risco referente as ameaças e ações do atacante
	Representa a zona de proteção referente aos alertas de prevenção e contramedidas

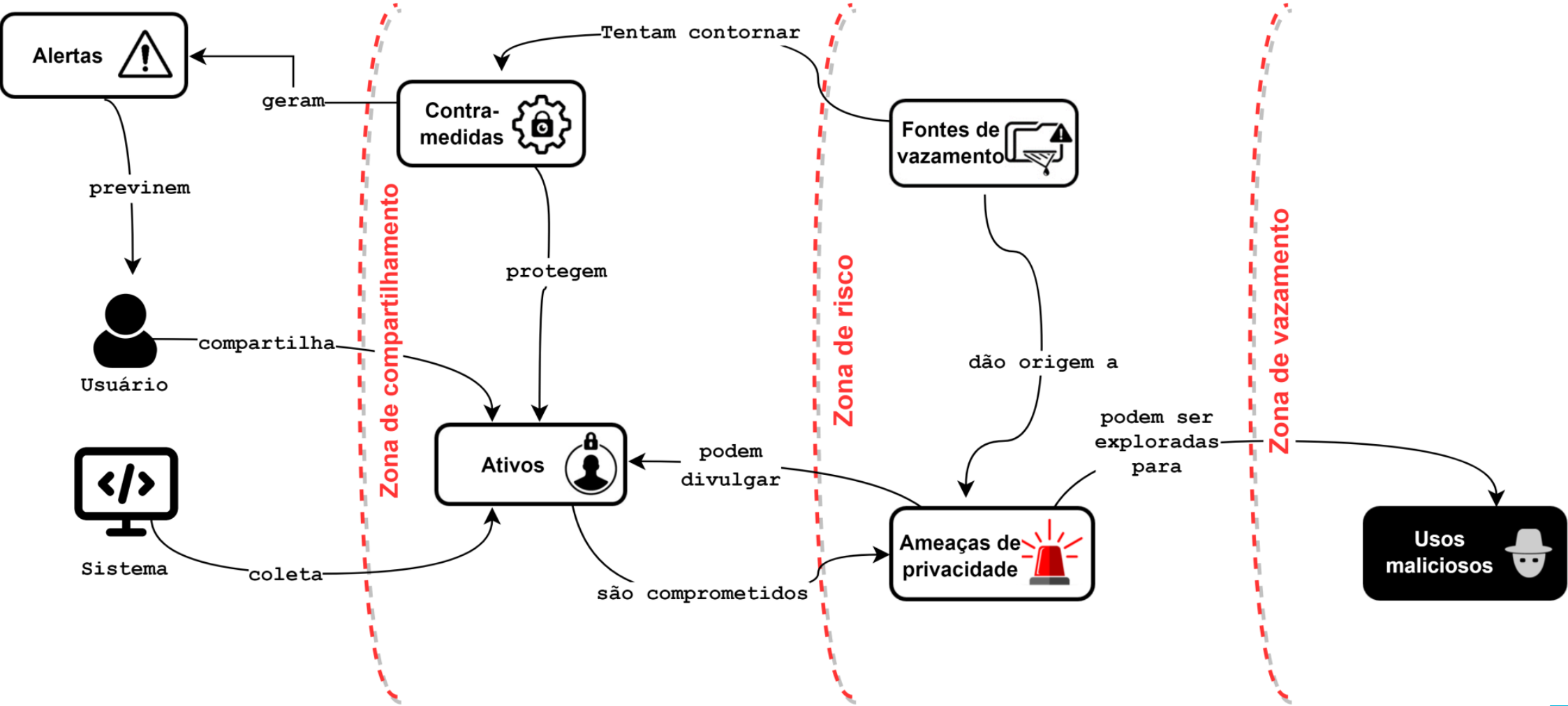
Versão 2 - Melhorias e Evolução

Criou-se o elemento “fontes de vazamento”. Indicar a fonte responsável pela ameaça traz uma complementação ao processo de modelagem da PTMOL e ajuda a refletir de forma mais correta sobre os usos maliciosos que aquela determinada fonte poderá produzir.



Novo elemento incluído no *template* de modelagem

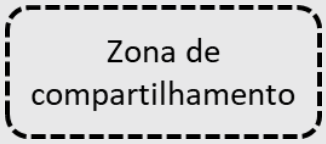
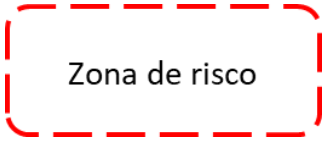
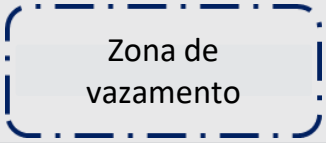
Versão 3 – Notação da linguagem



Versão 3 – Notação da linguagem

Notação	Descrição
	Algo relacionado ao alvo (usuário) que possui um valor pessoal
	Uma situação indesejável que pode colocar em risco os ativos do usuário.
	Ação que um agente malicioso executa para violar a privacidade de um usuário.
	Agentes maliciosos que pode estar infiltrados dentro ou fora da rede para violar a privacidade do usuário.

Versão 3 – Notação da linguagem

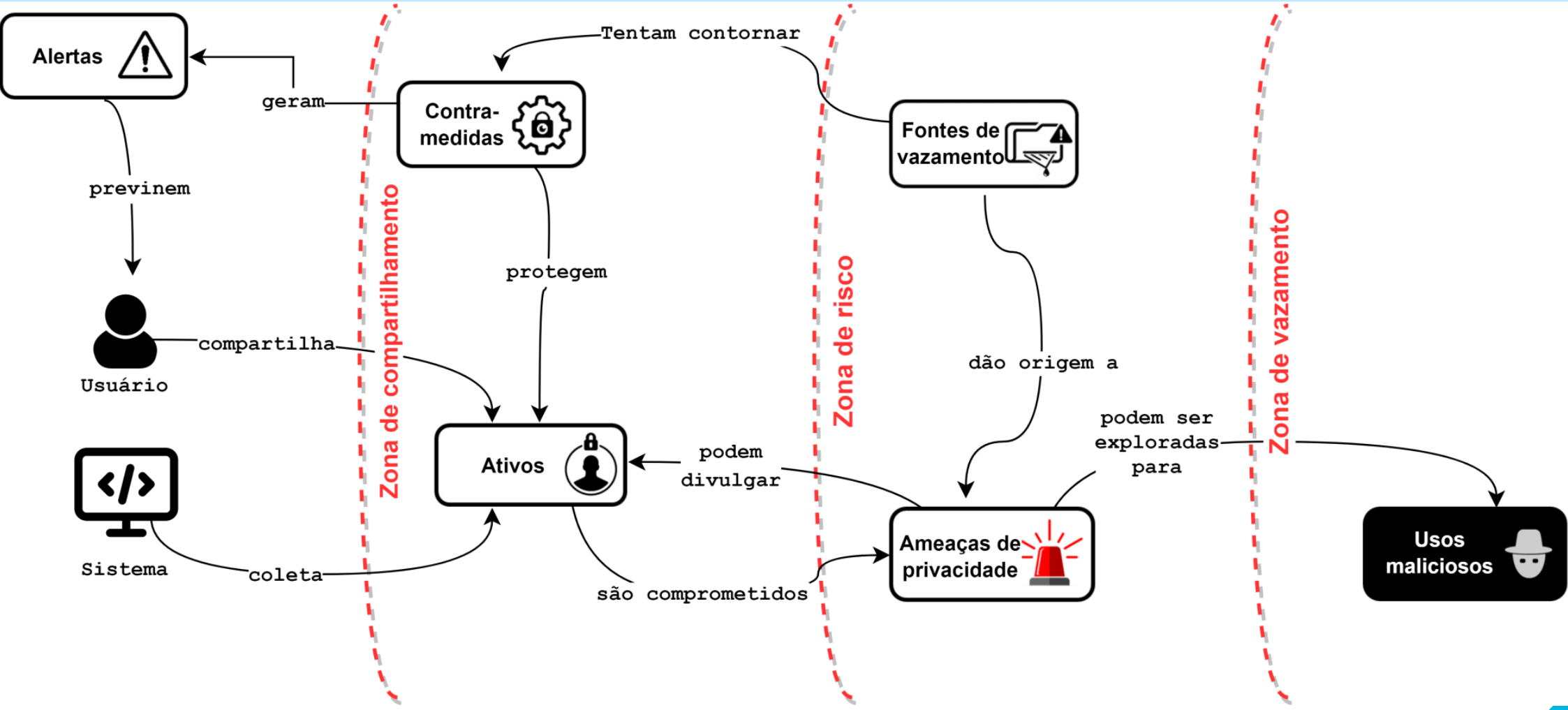
Notação	Descrição
	Representa um alerta do sistema para informar os usuários sobre qualquer ação com consequências importantes.
	Estratégia para mitigar ameaças de privacidade exploradas por agentes maliciosos
	Representa a zona de compartilhamento de ativos
	Representa a zona de risco referente as ameaças e ações do atacante
	Representa a porta de acesso indevido aos dados privados do usuário

Versão 3 - Melhorias e Evolução

Foi implementada uma subetapa complementar à etapa de identificação de contramedidas. Antes de iniciar essa fase, o designer deverá indicar para cada ameaça listada no *template* de modelagem, qual propriedade de privacidade a mesma poderia violar.

Ameaça de privacidade 	**Qual propriedade de privacidade pode ser violada?**						
	Desvinculação	**Anonimato**	**Negação plausível**	**Não detecção**	**Confidencialidade**	**Conscientização**	**Transparência**
Ameaça 1	X					X	
Ameaça 2		X					
Ameaça 3			X				X
...				X		X	
Ameaça n		X			X		

Versão 4 (atual) – Notação da linguagem



Template para classificação de ativos

Ativos	ATIVOS COMPARTILHADOS PELO USUÁRIO					
	Dado Textual		Dado multimídia			Dado geográfico
	Arquivo (PDF, DOC)	Texto livre	Foto	Vídeo	Áudio	Geolocalização
Ativo 1						
Ativo 2						
Ativo 3						
...						
Ativo n						
<Listar todos os ativos>	<Marcar com "X" a forma de compartilhamento do ativo>					

Regras de preenchimento

Template para classificação de ativos

Ativos	ATIVOS COLETADOS PELO SISTEMA	
	Dados de uso	Dados de relacionamento
Ativo 1		
Ativo 2		
Ativo 3		
...		
Ativo n		
<Listar todos os ativos>	<Marcar com "X" se o ativo pertencer a essa categoria>	<Marcar com "X" se o ativo pertencer a essa categoria>

Regras de preenchimento

Template para identificar ameaças, fontes de vazamento e usos maliciosos

Ativos 	Classificação do ativo	Ameaças de privacidade 	Fontes de vazamento 	Usos maliciosos 
O que deve ser protegido?	Ativo coletado ou compartilhado?	Que situações podem colocar em risco os ativos do usuário?	Quem são os agentes da ameaça?	Quais os usos maliciosos que podem afetar a privacidade?
Ativo 1	Valor pré-definido	Valor pré-definido	Valor pré-definido	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Classificar ativo>	<Associar ameaça [do catálogo] ao ativo>	<Indicar a fonte de vazamento>	<Prever usos maliciosos>

Especificação do tipo do valor do elemento

Regras de preenchimento

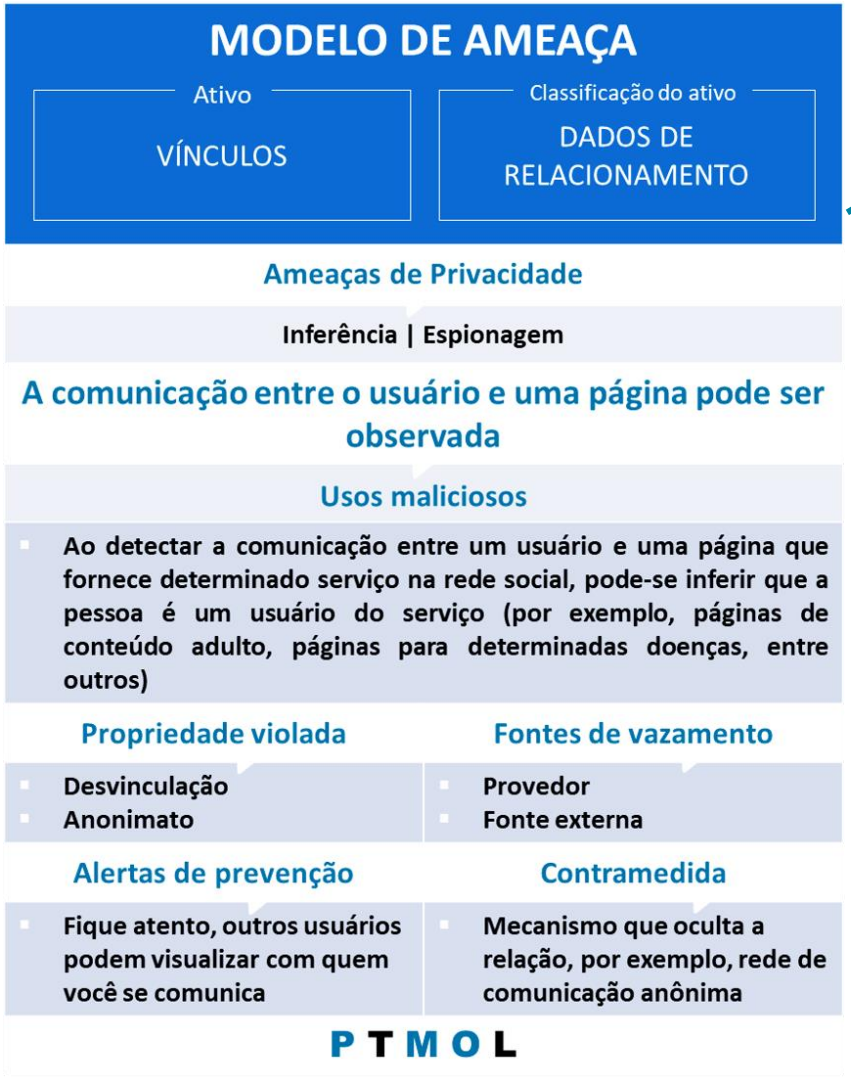
Template para prever contramedidas

Ativos 	Ameaças de privacidade 	Propriedade Violada	Contramedidas 	Alerta de prevenção 
O que deve ser protegido?	Que situações podem colocar em risco os ativos do usuário?	Quais propriedades de privacidade foram violadas?	Qual estratégia adotar para mitigar as ameaças?	Que alerta poderia ser emitido para informar o usuário sobre consequências para a sua privacidade.
Ativo 1	Valor pré-definido	Valor pré-definido	Valor livre	Valor livre
Ativo 2				
Ativo 3				
...				
Ativo n				
<Listar todos os ativos>	<Listar todas as ameaças>	<Indicar a propriedade violada>	<Prever contramedidas>	<Gerar um alerta em situações graves>

Especificação do tipo do valor do elemento

Regras de preenchimento

Template para gerar o modelo de ameaças



MODELO DE AMEAÇA

Ativo	Classificação do ativo
VÍNCULOS	DADOS DE RELACIONAMENTO

Ameaças de Privacidade

Inferência | Espionagem

A comunicação entre o usuário e uma página pode ser observada

Usos maliciosos

- Ao detectar a comunicação entre um usuário e uma página que fornece determinado serviço na rede social, pode-se inferir que a pessoa é um usuário do serviço (por exemplo, páginas de conteúdo adulto, páginas para determinadas doenças, entre outros)

Propriedade violada	Fontes de vazamento
▪ Desvinculação ▪ Anonimato	▪ Provedor ▪ Fonte externa

Alertas de prevenção	Contramedida
▪ Fique atento, outros usuários podem visualizar com quem você se comunica	▪ Mecanismo que oculta a relação, por exemplo, rede de comunicação anônima

P T M O L

Exemplo do resultado de um modelo de ameaças gerado pelo processo de modelagem da PTMOL

Apêndice F

Oráculos

Oráculos

ORÁCULO DESCRITIVO DO PRIMEIRO ESTUDO

Ativo	Forma de Compartilhamento	Descrição do problema	Ameaça
Nome	Texto livre	Coletar essa informação e fornecer/vender para entidades maliciosas que queiram mais informações sobre o usuário.	Divulgação de Informação
Nome	Texto livre	Perseguição da vítima através da busca pelo perfil da mesma em outras redes sociais;	Cyberstalking
Número de Telefone	Texto livre	Divulgação do número de telefone da vítima de forma pública em fóruns inadequados	Divulgação de Informação
Número de Telefone	Texto livre	Realizar chamadas para a vítima que configurem 'trote' de forma insistente; ou realizar chamadas insistentes para a vítima fingindo ser outra pessoa;	Cyberstalking
Email	Texto livre	Divulgação do email da vítima de forma pública em fóruns inadequados, ou utilização para criação de contas e consequentemente postagens de cunho inadequado.	Divulgação de Informação
Email	Texto livre	Realizar envio de diversos emails para a vítima, de forma insistente ou realizar chamadas insistentemente para a vítima, fingindo ser outra pessoa;	Cyberstalking
Foto de casa	Foto	Postagem de fotos da casa da vítima em outros ambientes da interwebs, como outras redes sociais;	Divulgação de Informação
Foto da casa	Foto	O Atacante poderia usar esse tipo de dado para extrair ou inferir informações pessoais, de membros familiares, ações cotidianas	Inferência
Vídeo da casa	Vídeo	Postagem de vídeos da casa da vítima em outros ambientes da interwebs, como outras redes sociais;	Divulgação de Informação
Video da casa	Video	Inferir informações pessoais como saber se mais alguém reside na casa, verificar quadros fotográficos, objetos pessoais, etc	Inferência
Endereço	Geolocalização	Divulgar para o público e mídia o endereço do usuário, no caso de ser uma figura pública, ou pessoas envolvidas em caso polêmico.	Divulgação de localização
Endereço	Texto livre	O atacante pode compartilhar o endereço para pessoas com o intuito de roubar/invadir a casa	Divulgação de informação
Endereço	Texto livre	Facilitar sequestros e roubos, contratação de serviços por assinatura.	Divulgação de localização
Endereço	Geolocalização	No caso de inferências essas informações podem ser utilizadas para que empresas possam divulgar os seus produtos para o usuário de acordo com as informações que foram coletadas pelas fotos	Inferências

Foto da casa	Foto	Comparar imagens com um banco de dados de imagens da cidade e descobrir o endereço da pessoa	Divulgação de localização
Vídeo da casa	Vídeo	Usar uma aplicação que transforma vídeos em imagens e então Comparar essas imagens com um banco de dados de imagens da cidade e descobrir o endereço da pessoa	Divulgação de localização

ORÁCULO DESCRITIVO DO SEGUNDO ESTUDO

Ativo	Classificação	ID Ameaça	Descrição do problema	Ameaça
NOME COMPLETO	Texto livre	01001	O atacante poderia usar esse dado para criar um pefil fake com o nome de perfil do usuario além de com essa e outras informaçoes poder criar uma conta em alguma rede social se passando pela pessoa.	Clonagem de perfil
NOME DE PERFIL	Texto livre	02001	O atacante poderia usar esse dado para criar um pefil fake com o nome de perfil do usuario além de com essa e outras informaçoes poder criar uma conta em alguma rede social se passando pela pessoa.	Clonagem de perfil
E-MAIL	Texto livre	03001	O atacante teria o endereço de e-mail e com essa informação só teria que conseguir mais informaçoes para realizar um rastramento de informações e também poderia realizar.	Reastreamento e interferencia
BIOGRAFIA PESSOAL	Texto livre	04001	Com a divulgação da biografia pessoal o atacante teria informações para fazer um rastreamento de informações para tentar ter acesso a senhas como a senha do e-mail e do perfil na rede social.	Divulgação de informações
FOTO DE PERFIL	Imagem	05001	Com a divulgação da foto de perfil o atacante poderia reconhecer o usuario e poderia usar para clonar o pefil em outra rede como o whatsapp para pedir dinheiro ao contatos do usuario já identificados pelo atacante.	Reconhecimento facil
VÍDEO	Vídeo	06001	Com a publicação de um video o atacante pode usar para identificar o lugar que o usuario frequenta e reconhecer outros usuarios presentes no video assim ele saberia quais pessoas frequentam determinado lugar ou que esporte gostam de praticar ou qualquer outra informação pessoal do usuario.	Reconhecimento facial,
LOCALIZAÇÃO	Geolocalização	07001	O atacante saberia que lugares o usuario frequenta onde mora ou trabalha, se por exemplo o atacante deseja realizar um ataque a empresa que usuario trabalha poderia sequestrar o usuario e o coagir ou ate mesmo usar engenharia social para extrair informações.	Divulgação de informações

Nº DO CARTÃO	Textual	08001	O atacante poderia se passar pelo usuario e usar os dados do cartão para fazer compras no nome do usuario.	Roubo de identidade
ENDEREÇO	Textual	09001	O atacante saberia onde o usuario mora, isso seria uma brecha para que podesse realizar engenharia social contra o usuario.	Divulgação de informações
BIOGRAFIA PESSOAL	Texto livre	16001	Com a divulgação da biografia pessoal o atacante teria informações para fazer um rastreamento de informações para tentar ter acesso a senhas como a senha do e-mail e do perfil na rede social.	Ameaça a reputação,
FOTO DE PERFIL	Imagem	17001	Com a divulgação da foto de perfil o atacante poderia reconhecer o usuario e poderia usar para clonar o pefil em outra rede como o whatsapp para pedir dinheiro ao contatos do usuario já identificados pelo atacante.	Clonagem de perfil
VÍDEO	Vídeo	18001	Com a publicação de um video o atacante pode usar para identificar o lugar que o usuario frequenta e reconhecer outros usuarios presentes no video assim ele saberia quais pessoas frequentam determinado lugar ou que esporte gostam de praticar ou qualquer outra informação pessoal do usuario.	Divulgação de informações
Localização	Geolocalização	19002	O atacante poderia espionar a vitima por meio de suas publicações , deixando assim a vítima vulnerável a vários riscos .	espionagem ou monitoramento
Fotos	Fotos	20002	O atacante poderia espionar a vitima por meio de suas publicações , deixando assim a vítima vulnerável a vários riscos .	espionagem ou monitoramento
Vídeos	Vídeo	21002	O atacante poderia espionar a vitima por meio de suas publicações , deixando assim a vítima vulnerável a vários riscos .	espionagem ou monitoramento
EMAIL	Texto livre	23002	Por meio dos dados pessoais possibilita o atacante a usar as informações e se passar pela vítima para realizar ações maliciosas .	Clonagem
BIOGRAFIA PESSOAL	Texto livre	24002	Por meio dos dados pessoais possibilita o atacante a usar as informações e se passar pela vítima para realizar ações maliciosas .	Clonagem
Email	Texto livre	27003	Salvar o email para fins maliciosos, divulgar para compartilhamento de arquivos duvidosos ou propagandas.	Divulgação de informação

BIOGRAFIA PESSOAL	Texto livre	29002	Por meio dos dados pessoais possibilita o atacante a usar as informações e se passar pela vítima para realizar ações maliciosas .	Cyberstalking
VÍDEO	VÍDEO	35003	Usar da mesma forma que uma foto, pegando partes do vídeo para desbloquear contas ou tentar invadir aplicativos, caso em local aberto, tentar perseguir a pessoa de acordo com as informações mostradas no vídeo, tirar o vídeo de contexto e usando para fins maliciosos.	Cyberstalking
VÍDEO	VÍDEO	36003	Usar da mesma forma que uma foto, pegando partes do vídeo para desbloquear contas ou tentar invadir aplicativos, caso em local aberto, tentar perseguir a pessoa de acordo com as informações mostradas no vídeo, tirar o vídeo de contexto e usando para fins maliciosos.	Ameaça de reputação
Localização	Geolocalização	42004	Utilizar a localização para localizar o endereço ou o local que o usuário se encontra	Rastreamento e Inferência
Número do cartão	Textual	43004	Ter acesso aos dados da conta bancária e outras informações do usuário	Divulgação de informações
FOTO	Mídia	45006	Realizar perfil falsos com a foto de perfil e tenta engana familiares e amigos, tambem usa essa foto para acessar reconhecimento facial	Clonagem de perfil