VINÍCIUS CAMARGO ANDRADE

PROCESSO DE DESENVOLVIMENTO DE SOFTWARE BASEADO NOS PRINCÍPIOS DE PRIVACY BY DESIGN

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática.

Curitiba
2024

VINÍCIUS CAMARGO ANDRADE

PROCESSO DE DESENVOLVIMENTO DE SOFTWARE BASEADO NOS PRINCÍPIOS DE PRIVACY BY DESIGN

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Doutor em Informática.

Área de concentração: Ciência da Computação

Orientadora: Profª. Drª. Andreia Malucelli
Coorientadora: Profª. Drª. Cinthia O. A. Freitas

Curitiba
2024

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Luci Eduarda Wielganczuk – CRB 9/1118

A553p 2024

Andrade, Vinícius Camargo
Processo de desenvolvimento de software baseado nos princípios de *privacy by design* / Vinícius Camargo Andrade ; orientadora: Andreia Malucelli ; coorientadora: Cinthia O. A. Freitas. – 2024.
xxii, 316 f. : il. ; 30 cm

Tese (doutorado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2024
Bibliografia: f. 161-176

1. Software – Desenvolvimento. 2. Computadores – Medidas de segurança. I. Malucelli, Andreia. II. Freitas, Cinthia O. A. III. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática. IV. Título.

CDD. 21. ed. – 005.1

Pontifícia Universidade Católica do Paraná
Escola Politécnica
Programa de Pós-Graduação em Informática

Curitiba, 22 de maio de 2024.

40-2024

DECLARAÇÃO

Declaro para os devidos fins, que **Vinicius Camargo Andrade** defendeu a tese de Doutorado intitulada "**PROCESSO DE DESENVOLVIMENTO DE SOFTWARE BASEADO NOS PRINCÍPIOS DE PRIVACY BY DESIGN"**, na área de concentração Ciência da Computação no dia 26 de abril de 2024, no qual foi aprovado.

Declaro ainda, que foram feitas todas as alterações solicitadas pela Banca Examinadora, cumprindo todas as normas de formatação definidas pelo Programa.

Por ser verdade firmo a presente declaração.

Documento assinado digitalmente
gov.br
EMERSON CABRERA PARAISO
Data: 23/05/2024 17:43:27-0300
Verifique em https://validar.iti.gov.br

_____
Prof. Dr. Emerson Cabrera Paraiso
Coordenador do Programa de Pós-Graduação em Informática

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos a todos que contribuíram para a realização deste trabalho. Em primeiro lugar, agradeço a Deus pela saúde, sabedoria e discernimento que me concedeu ao longo deste processo.

Aos meus pais, Paulo Roberto de Andrade e Milze de Fátima Camargo Andrade, expresso minha gratidão pela vida e pelo apoio incondicional que sempre me ofereceram, especialmente nos momentos mais desafiadores.

À minha amiga, confidente, companheira de vida, e uma das pesquisadoras mais talentosas que conheço, Ana Cristina Munaro, agradeço pelo constante suporte, sugestões e ajuda que foram fundamentais para me motivar, refletir e definir os rumos da pesquisa.

Especialmente às minhas orientadoras, Profa. Dra. Andreia Malucelli e Profa. Dra. Cinthia Obladen de Almendra Freitas, pelo profissionalismo e dedicação em todas as etapas deste grande desafio.

Não menos importante, à Profa. Dra. Sheila Reinehr, que, juntamente com minhas orientadoras, forneceu valiosas contribuições que enriqueceram ainda mais o presente trabalho.

À Profa Dra. Lina Maria Garces Rodriguez, ao Prof. Dr. Vinícius Borges Fortes e, novamente, à Profa. Dra. Sheila Reinehr pela composição da banca da Defesa de Doutorado.

Ao Prof. Dr. Paulo Sergio Macuchen Nogas, que não mediu esforços em me auxiliar nas análises dos dados quantitativos da pesquisa.

Aos amigos Richard Duarte Ribeiro, Luis Renato dos Santos, Rafael dos Passos Canteri e Cesar Mauricio Chauchuty, agradeço não apenas pelas valiosas contribuições técnicas, mas também pelos momentos de descontração e incentivo ao longo do período doutoral.

À Flávia Beuting e à Lilian Vicente, que estiveram à frente da secretaria do Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná, meu reconhecimento pelo apoio prestado ao longo dos anos.

E, por fim, à Pontifícia Universidade Católica do Paraná, especialmente ao Programa de Pós-Graduação em Informática (PPGIa), pela oportunidade de cursar esta pós-graduação de alto nível.

What we do in life, echoes in eternity!

Marcus Aurelius.

RESUMO

A coleta, processamento, armazenamento e compartilhamento de dados de usuários auxiliam os provedores de serviços a entender as preferências dos usuários, possibilitando a oferta de produtos e serviços personalizados, além de contribuir para a tomada de melhores decisões de negócios. Entretanto, o uso irresponsável dos dados pessoais coloca em risco a privacidade dos titulares de dados. Este risco ocorre não apenas após o software/app/sistema estar em pleno funcionamento, mas desde as etapas iniciais do desenvolvimento do software. Com o intuito de integrar a privacidade e a proteção de dados pessoais durante todas as fases do desenvolvimento do software, o *Privacy by Design* (PbD) foi criado e, recentemente, leis e regulamentos têm sido estabelecidos, como o *General Data Protection Regulation* (GDPR), na União Europeia, e a Lei Geral de Proteção de Dados Pessoais (LGPD), no Brasil. Tanto o GDPR quanto a LGPD mencionam a importância de salvaguardar os dados pessoais dos titulares em todas as etapas de desenvolvimento de software. Porém, o alto nível de abstração dos princípios do PbD dificulta sua aplicação. Este trabalho tem como objetivo propor um processo de desenvolvimento de software para auxiliar equipes na implementação dos princípios do PbD. Esta pesquisa foi realizada por meio da *Design Science Research Methodology*, que é composta por seis etapas: identificar o problema e motivação; definir os objetivos para uma solução; projetar e desenvolver o processo, papel e artefatos propostos; demonstrar o processo, papel e artefatos por meio de avaliações empíricas qualitativas junto aos especialistas; avaliar os resultados qualitativos das avaliações a fim de aprimorar o processo, papel e artefatos propostos; e comunicar os resultados por meios científicos. Os resultados evidenciam que o processo, papel e artefatos são significativos e podem auxiliar equipes de desenvolvimento de software na implementação de soluções para problemas relacionados à violação do direito de proteção de dados pessoais desde as primeiras etapas do desenvolvimento do software, conforme abordam os princípios do PbD.

Palavras-chaves: Processo de Software, *Privacy by Design*, Padrões de Privacidade.

ABSTRACT

Collecting, processing, storing, and sharing user data helps service providers understand user preferences, enabling them to offer personalized products and services and contribute to making better business decisions. However, the irresponsible use of personal data puts the privacy of data subjects at risk. This risk occurs not only after the software/app/system is fully operational but also from the initial stages of software development. In order to integrate privacy and personal data protection during all phases of software development, Privacy by Design (PbD) was created, and recently, laws and regulations have been established, such as the General Data Protection Regulation (GDPR), in the European Union, and the General Personal Data Protection Law (LGPD), in Brazil. GDPR and LGPD mention the importance of safeguarding data subjects' personal data at all stages of software development. However, the high level of abstraction of PbD principles makes their application difficult. This work proposes a software development process to assist teams in implementing PbD principles. This research was carried out using the Design Science Research Methodology, which is composed of six steps: identify problem and motivate; define objectives of a solution; design and develop the proposed process, paper, and artifacts; demonstrate the process, role, and artifacts through qualitative empirical assessments with experts; evaluate the qualitative results of the evaluations in order to improve the proposed process, role, and artifacts; and communicate results through scientific means. The results show that the process, role, and artifacts are significant and can assist software development teams in implementing solutions to problems related to violations of the right to personal data protection from the first stages of software development, as addressed by PbD principles.

Keywords: Software Process, Privacy by Design, Privacy Patterns.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

APEC	Asia-Pacific Economic Cooperation
CEP	Comitê de Ética em Pesquisa
CONEP	Conselho Nacional de Saúde
CPF	Cadastro de Pessoa Física
CPL	Cross Product Leader
DPO	Data Protection Officer
DSRM	Design Science Research Methodology
EU	European Union
FIPP	Fair Information Practice Principles
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
GPS	Global Privacy Standard
HIPAA	Health Insurance Portability and Accountability Act
ICC	Intraclass Correlation Coefficient
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISSO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados Pessoais
MOAB	Mother of All Breaches

NSA	Agência Nacional de Segurança
OECD	Organisation for Economic Cooperation and Development
ONU	Organização das Nações Unidas
P	Proposição
P3P	Privacy Preferences Project
PA	Ponto de Análise
PAGE	Policy AutoGeneration in Eclipse
PbD	Privacy by Design
PDSOP	Processo de Desenvolvimento de Software Orientado à Privacidade
PEAR	Privacy Enhancing Architecture
PET	Privacy-Enhancing Technologies
PII	Personally Identifiable Information
PIX	Sistema de Pagamento Instantâneo
PKB	Privacy Knowledge Base
PM	Product Manager
PO	Product Owner
POC	Proof of Concept
POSD	Privacy Oriented Software Development
PUCPR	Pontifícia Universidade Católica do Paraná
QP	Questão de Pesquisa
RSL	Revisão Sistemática da Literatura

SAFe	Scaled Agile Framework
SWEBOK	Software Engineering Body of Knowledge
TAM	Technology Acceptance Model
TCLE	Termo de Consentimento Livre e Esclarecido
TCUD	Termo de Compromisso de Utilização de Dados
TI	Tecnologia da Informação
UKDPA	UK Data Protection Act
UML	Unified Modeling Language
UP	Unified Process
XP	eXtreme Programming

CAPÍTULO 1 - INTRODUÇÃO

Em 2014, a Organização das Nações Unidas (ONU) publicou uma resolução na qual defende que um indivíduo deve ter garantidos os mesmos direitos, seja off-line ou no mundo digital, incluindo-se o direito à privacidade (CHANDER; LAND, 2014). Neste mesmo documento, a ONU convocou os países a "revisar seus procedimentos, práticas e legislação em relação à vigilância de comunicações, sua interceptação e coleta de dados pessoais" (CHANDER; LAND, 2014). Isso aconteceu principalmente após as revelações de vigilância em massa, relatadas por um ex-funcionário que prestava serviço à Agência Nacional de Segurança (NSA, em inglês) dos Estados Unidos da América, que colocaram a privacidade na vanguarda do debate político e social e revelaram graves violações de privacidade. A privacidade pode ser definida como o direito do indivíduo de acessar e controlar seus dados pessoais no que diz respeito à sua coleta, uso e transferência pelos meios de comunicação (BORITZ; WON; SUNDARRAJ, 2008).

Apesar de toda a importância dada a este tema, problemas relacionados à violação do direito à privacidade de dados pessoais continuam ocorrendo. Em 2012, por exemplo, aconteceu o vazamento de informações da empresa LinkedIn[1] afetando 165 milhões de usuários, e em 2013 aconteceram vazamentos do Yahoo[2], atingindo 3 bilhões de usuário e do MySpace[3], impactando 360 milhões de usuários.

Mesmo com este cenário, uma parcela dos usuários de softwares e empresas em diversos domínios só compreenderam a seriedade da questão em 2018, quando se revelou o escândalo envolvendo as empresas Facebook[4] e Cambridge Analytica[5] relacionado à coleta e uso de dados pessoais, afetando um total de 87 milhões de usuários da rede social (CADWALLADR; GRAHAM-HARRISON, 2018; ROSENBERG, 2018; TEAM, 2018).

[1] Site LinkedIn: http://www.linkedin.com
[2] Site Yahoo: https://yahoo.com
[3] Site MySpace: https://myspace.com
[4] Site Facebook: https://www.facebook.com
[5] Site Cambridge Analytica: https://cambridgeanalytica.org

Entretanto, os problemas de violação de privacidade de dados pessoais não pararam. Em 2019 a plataforma de música Deezer[6] sofreu com vazamento de dados a qual expôs mais de 220 milhões de contas de usuários (INFOMONEY, 2023). Em 2021 a Twitch[7], plataforma de *streaming* da Amazon[8], sofreu vazamento de 128 gigabytes de dados pessoais de *streamers* (BROWNING, 2021; TIDY; MOLLOY, 2021). Em 2023 foi descoberto que a Microsoft[9] acidentalmente expôs 38 terabytes de informações pessoais, como senhas, chaves privadas e mensagens internas do Microsoft Teams[10] (BEN-SASSON; GREENBERG, 2023). Por fim, em 2024, ocorreu o vazamento de dados mais significativo da história, conhecido como “Mãe de Todas as Violações” (MOAB, em inglês *Mother of All Breaches*), com 26 bilhões de registros expostos de usuários de diversos serviços, como Tencent, Weibo, MySpace, X (antigo Twitter), entre outros (PETKAUSKAS, 2024).

No Brasil, em 2018, ocorreu um vazamento de dados do Banco Inter[11], afetando 19.961 correntistas. Na ocasião, o banco teve que pagar R$ 1,5 milhão em indenizações (REDAÇÃO VEJA, 2018). Posteriormente, em janeiro de 2021 houve o maior vazamento de dados da história brasileira, no qual 223 milhões de brasileiros foram impactados com a exposição dos números de seus CPFs. Este número ultrapassa o do tamanho atual da população brasileira pelo fato de nos dados vazados existirem CPFs relacionados à pessoas falecidas (ROHR, 2021). E, em 2022, o Banco Central do Brasil anunciou o vazamento de mais de 130 mil chaves de pagamento instantâneo, conhecido como PIX[12], as quais estavam relacionadas aos nomes dos usuários, CPFs, instituições de relacionamento, agência, conta e tipo de conta, além da data de criação do PIX (MALAR, 2022).

Todas as plataformas que foram alvo de incidentes ou escândalos possuem algo em comum: coletam, processam, armazenam e compartilham um grande volume de dados pessoais de seus usuários com o intuito de fornecerem produtos, serviços e publicidade de modo personalizado por meio do conhecimento de suas preferências, comportamentos, gostos, histórico, localização, entre outros. Em contrapartida, a

---

[6] Site Deezer: https://www.deezer.com
[7] Site Twitch: https://www.twitch.tv
[8] Site Amazon: https://www.amazon.com
[9] Site Microsoft: https://www.microsoft.com
[10] Site Microsoft Teams: https://www.microsoft.com/microsoft-teams
[11] Site Banco Inter: https://www.bancointer.com.br
[12] PIX: Sistema de pagamento instantâneo criado pelo Banco Central do Brasil (INFOMONEY, 2022).

privacidade dos titulares destes dados é frequentemente colocada em risco (SUPHAKUL; SENIVONGSE, 2017).

Além de destacar a exposição da privacidade dos titulares de dados após o software/app/sistema estar em pleno funcionamento, é importante ressaltar que essa vulnerabilidade permeia todas as fases do desenvolvimento do software. Essa preocupação ganha ainda mais relevância no contexto das organizações de desenvolvimento de software, onde os processos ágeis de desenvolvimento são amplamente empregados devido às suas diversas vantagens sobre os modelos tradicionais. Esses processos não apenas enfatizam a entrega frequente de software, a colaboração com o cliente e a capacidade de resposta às mudanças, mas também promovem a melhoria contínua, incentivam equipes autogeridas e favorecem avaliações internas constantes. Nesse sentido, a consideração da privacidade dos titulares de dados deve ser integrada de forma abrangente em todas as etapas do desenvolvimento ágil, desde a concepção inicial até a entrega final do produto (GILL; HENDERSON-SELLERS; NIAZI, 2018; PFLÜGLER; WIESCHE, 2018; REDDY; KUMAR, 2020). Entretanto, os processos ágeis são criticados por não possuírem práticas explícitas para requisitos não funcionais, como a proteção de dados pessoais, usabilidade, segurança, portabilidade, manutenção e desempenho (CURCIO *et al.*, 2018). Neste caso, os requisitos não funcionais deveriam ser discutidos com maior profundidade, a fim de implementar soluções adequadas desde as primeiras versões entregues ao cliente, minimizando as chances de ocorrerem problemas, principalmente de violação de privacidade e ausência de segurança de dados (MIRZA; DATTA, 2019; REDDY; KUMAR, 2020).

Ao tentar solucionar os recorrentes problemas relacionados à proteção de dados e privacidade de seus cidadãos decorrentes do uso de softwares, alguns países desenvolveram ou alteraram suas leis e regulamentos para controlar as operações relacionadas aos dados pessoais. Alguns exemplos são o regulamento da União Europeia, que está em vigor desde o mês de maio de 2018, denominado *General Data Protection Regulation (GDPR)* (EU, 2016); e mais recentemente, a lei brasileira sancionada em 14 de agosto de 2018, em vigor desde o dia 18 de setembro de 2020, denominada Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a). Além disso, Cavoukian (2009a) propôs o conceito do *Privacy by Design* (PbD) com 7 (sete) princípios que enfatizam de maneira proativa à privacidade e à proteção de

dados pessoais durante todo o ciclo de vida do software, desde a sua concepção até a sua finalização.

Tanto o GDPR quanto a LGPD deixam explícita a exigência de salvaguardar os dados pessoais dos titulares durante todo o ciclo de desenvolvimento de software. Para isto, os princípios do PbD podem ser aplicados pelos provedores de serviços, os quais devem modificar seus métodos de aquisição, gerenciamento e processamento de dados privados, bem como o monitoramento de violações de dados, notificações e preparações de planos de prevenção, desde as primeiras etapas do projeto. Estas exigências procuram fornecer aos titulares dos dados maiores informações de como seus dados pessoais estão sendo utilizados, dando-lhes a opção de revogar as permissões, se assim preferirem (BRASIL, 2018a; EU, 2016).

Apesar da possibilidade da implementação dos princípios do PbD em projetos de software, o PbD sofre inúmeras críticas devido aos seus princípios possuírem um nível alto de abstração, dificultando a implementação por parte da tecnologia. A própria autora dos princípios do PbD cita que “o próximo estágio da evolução do PbD é traduzir seus 7 Princípios Fundamentais em requisitos, especificações, padrões, melhores práticas e critérios de desempenho operacional mais prescritivos” (CAVOUKIAN, 2012a).

Ciente das críticas do alto grau de abstração dos princípios do PbD, alguns trabalhos tentaram aproximar os princípios das atividades práticas na Engenharia de Software. Hadar *et al*. (2018) e Baldassarre *et al.* (2020) mencionam o desafio de estabelecer diretrizes e ferramentas que contemplem os princípios do PbD e auxiliem o time de desenvolvimento de software a projetar e implementar sistemas que façam valer o direito à privacidade. As pesquisas de Gürses e Del Alamo (2016), Alshammari e Simpson (2017) e Peixoto *et al.* (2023), descrevem a falta de metodologias que apoiem engenheiros de software na aplicação dos princípios do PbD em atividades práticas da Engenharia de Software. O trabalho de Veseli *et al.* (2019) relata que o PbD deixa como uma questão a ser respondida como os princípios de privacidade serão traduzidos em requisitos de engenharia e Bu *et al.* (2020) evidencia que as pesquisas existentes entre a implementação do PbD e os fatores de decisões individuais dos engenheiros de softwares são inconclusivas, pois o PbD não é adotado extensivamente nas práticas de proteção de dados pessoais na indústria de desenvolvimento de software.

Apesar da ausência de métodos, diretrizes e ferramentas que auxiliem engenheiros de software a implementar os princípios da abordagem PbD na Engenharia de Software não ser um problema recente, ele ganhou notoriedade nos últimos anos com o GDPR. Porém, a dificuldade em aplicar os princípios do PbD em atividades práticas da Engenharia de Software resulta, não só na não conformidade com a legislação, mas também na não confiabilidade dos produtos gerados, pois tendem a ser mais suscetíveis a problemas relacionados à violação de privacidade, como por exemplo, vazamento de dados pessoais.

Neste contexto, surge a seguinte questão de pesquisa: **como apoiar equipes de desenvolvimento de software na implementação dos princípios do *Privacy by Design*?**

1.1 Objetivos

O objetivo geral desta pesquisa é **propor um processo de desenvolvimento de software para auxiliar equipes na implementação dos princípios do *Privacy by Design*.**

Para atingir o objetivo geral desta pesquisa, os seguintes objetivos específicos foram definidos:

i. Criar um repositório de instâncias de padrões de privacidade;
ii. Mapear os padrões de privacidade aos princípios fundamentais do PbD;
iii. Conceber um processo que considere os princípios fundamentais do PbD;
iv. Avaliar o processo proposto.

1.2 Delimitação de escopo

A presente pesquisa concentra-se na concepção de um processo de software destinado a auxiliar equipes de desenvolvimento na integração efetiva de requisitos de privacidade desde as fases iniciais do ciclo de desenvolvimento. O escopo desta pesquisa não impõe restrições quanto à adoção de um processo de desenvolvimento específico, permitindo que diferentes organizações adaptem o processo proposto em conjunto com suas práticas existentes.

A flexibilidade na integração visa facilitar a aceitação e a implementação eficaz em ambientes diversos, reconhecendo as particularidades e variações nos métodos de desenvolvimento utilizados pelas organizações.

É relevante destacar que este processo não tem como objetivo abordar legislações específicas sobre privacidade de dados pessoais, não estabelecendo diretrizes vinculadas às regulamentações particulares. A intenção é que as organizações usuárias do processo considerem e atendam às exigências legais pertinentes à sua região de atuação.

O foco da pesquisa é fornecer uma estrutura adaptável que incorpore boas práticas de privacidade, permitindo a conformidade com regulamentações específicas conforme necessário. Dessa forma, a pesquisa busca oferecer uma abordagem genérica e escalável, proporcionando flexibilidade para acomodar as nuances legais que podem variar entre diferentes jurisdições.

1.3 Estrutura do documento

O Capítulo 1 apresenta ao leitor o posicionamento desta pesquisa perante o estado da arte, além de definir a questão de pesquisa, objetivos e delimitar o tema associado à privacidade e proteção de dados pessoais e desenvolvimento de software.

O Capítulo 2 engloba a revisão da literatura de estudos primários e livros fundamentais sobre os temas de processos de desenvolvimento de software e princípios da privacidade de dados pessoais.

O Capítulo 3 descreve a estruturação desta pesquisa em relação ao seu posicionamento metodológico. A estrutura inclui a estratégia de pesquisa baseada nas atividades da *Design Science Research Methodology* (DSRM), proposto por Peffers *et al.* (2007), e a seleção dos métodos de pesquisa para realizar o estudo de caso múltiplo e a avaliação do processo.

O Capítulo 4 aborda a Revisão Sistemática da Literatura (RSL) sobre os avanços da Engenharia de Software em relação aos princípios fundamentais do *Privacy by Design*. São apresentados os protocolos seguidos, os estudos primários selecionados, extração de dados, resultados obtidos, ameaças à validade da revisão, além dos estudos relacionados com esta pesquisa.

O Capítulo 5 discorre sobre os estudos de caso realizados com diferentes organizações a fim de compreender como a privacidade dos dados pessoais está sendo integrada ao processo de desenvolvimento de software. Neste capítulo são detalhados o protocolo do estudo, questões de pesquisa, proposições, unidades de análise, recrutamento, pontos de análise, ameaças à validade do estudo e as conclusões obtidas a partir dos resultados.

O Capítulo 6 descreve a caracterização do processo, papel e artefatos propostos, sendo o objeto principal desta pesquisa. Além disso, exemplos de aplicação do processo proposto foram delineados, demonstrando sua integração harmoniosa com práticas consolidadas de desenvolvimento de software adotadas pelas organizações.

O Capítulo 7 discute a avaliação do processo. Esta avaliação permite avaliar e aperfeiçoar os artefatos sob o ponto de vista de especialistas em proteção de dados pessoais e desenvolvimento de software.

Por fim, o Capítulo 8 finaliza o trabalho destacando sua relevância, contribuições e limitações, além de apresentar os trabalhos futuros.

1.4 Considerações sobre o capítulo

Este capítulo introduziu o tema de privacidade de dados, apresentando sua importância e, ao mesmo tempo, relatando alguns incidentes e escândalos ocorridos nos últimos anos com o vazamento de dados pessoais. Visando a proteção dos titulares de dados, abordaram-se algumas leis e regulamentos que estão sendo escritas por diversos países, entre eles, o *General Data Protection Regulation (GDPR)* (EU, 2016) e a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a). Ambas não só discutem a privacidade de dados, mas também fornecem como solução a implementação do *Privacy by Design* (PbD) em projetos de software. Entretanto, esta não é uma tarefa simples, pois como apresentado por diversos autores, o PbD possui princípios abstratos demais para serem implementados como uma atividade prática da Engenharia de Software.

Neste sentido, foram apresentados problemas, limitações, motivações e lacunas sobre a implementação dos princípios do *Privacy by Design* na Engenharia de Software, além de alguns trabalhos que tentam preenchê-las, porém estes trabalhos descrevem estratégias e táticas consideradas amplas e vagas para serem

aplicadas na prática. Por fim, foram apresentados os objetivos, delimitação de escopo e a estrutura do documento desta pesquisa.

CAPÍTULO 2 - REVISÃO DA LITERATURA

Este capítulo apresenta os conceitos e definições essenciais acerca da fundamentação teórica dos temas utilizados para o desenvolvimento desta pesquisa. A Seção 2.1 aborda o conceito de processos de software, discorrendo sobre processos tradicionais e ágeis da Engenharia de Software. A Seção 2.2 introduz o conceito de privacidade de dados pessoais, discorrendo sobre os princípios do *Privacy by Design*, Estratégias de Hoepman, ISSO/IEC 29100:3011 e Padrões de Privacidade de Dados Pessoais. Por fim, a Seção 2.3 destaca as considerações finais do capítulo.

2.1 Processos Ágeis de Software

Na década de 1960, com o fortalecimento da indústria de hardware, a demanda por softwares cada vez mais complexos tornou-se eminente. Porém, nesta época, a Engenharia de Software ainda dava seus primeiros passos, o que gerou a conhecida “crise do software” (DIJKSTRA, 1972).

Alguns dos fatores que ocasionaram a crise do software, segundo Dijkstra (1972), foram: projetos não respeitavam o cronograma estabelecido, orçamentos eram frequentemente desrespeitados, produto final tinham baixa qualidade e/ou não atendiam os requisitos, processos não eram gerenciáveis e eram difíceis de manter e/ou evoluir, entre outros. Royce, ao observar estes problemas, propôs o primeiro modelo do processo de desenvolvimento de software, que ficou conhecido como “Modelo Cascata” (ROYCE, 1970), devido ao seu encadeamento entre as fases, e os seus principais estágios procuraram refletir as atividades fundamentais do desenvolvimento, que são: requisitos de sistema, requisitos de software, análise, projeto de programação, codificação, testes e operação.

Entretanto, notou-se que a própria natureza sequencial e sistemática do Modelo Cascata era impraticável, pois alterações no escopo do projeto após o seu início causavam enormes impactos ao produto final. Assim, surgiram variações do modelo ao longo do tempo a fim de desenvolver softwares de modo dinâmico e ágil, realizando entregas parciais do sistema ao cliente, o que possibilita obter *feedbacks* sobre o

produto que receberam e, consequentemente, um maior controle de mudanças e riscos no projeto (POPPENDIECK; POPPENDIECK, 2003; WAZLAWICK, 2019).

Após anos de evolução, surgiram os processos ágeis de desenvolvimento que seguem uma filosofia diferente dos modelos prescritivos. Em vez de apresentar fases a serem executadas, como nos modelos tradicionais, possuem foco nos valores humanos e sociais. Princípios estes que foram colocados no Manifesto Ágil (CUNNINGHAM, 2001; WAZLAWICK, 2019).

O Manifesto Ágil, criado em 2001, foi assinado por 17 desenvolvedores da área que se reuniram com o intuito de discutir uma alternativa aos processos de desenvolvimento de software orientados à documentação. Como consequência, foram definidos 4 valores do Manifesto Ágil (CUNNINGHAM, 2001):

1. Indivíduos e interações estão acima de processos e ferramentas;
2. Software funcional está acima de documentação compreensível;
3. Colaboração do cliente está acima de negociação de contrato;
4. Responder às mudanças está acima de seguir um plano.

Os valores do manifesto não indicam que os modelos ágeis não valorizam processos, documentações, contratos e planos, mas demonstram que estes elementos terão um maior valor quando os indivíduos, interações, colaborações com o cliente e respostas às mudanças também forem consideradas relevantes, pois, de nada adiantará processos e software bem estruturados e documentados se não satisfazem os requisitos do cliente ou não funcionam corretamente princípios (CUNNINGHAM, 2001).

Além dos 4 valores, o Manifesto Ágil possui 12 princípios (CUNNINGHAM, 2001):

1. Nossa maior prioridade é satisfazer o cliente por meio da entrega rápida e contínua de software de valor;
2. Mudanças nos requisitos são bem-vindas, mesmo em fases tardias do desenvolvimento. Processos Ágeis utilizam a mudança como um diferencial competitivo para o cliente;
3. Entregar software em funcionamento com frequência, com intervalos que variam de duas semanas a dois meses, com uma preferência por intervalos mais curtos;

4. Administradores e desenvolvedores devem trabalhar juntos diariamente durante todo o desenvolvimento do projeto;
5. Construir projetos em torno de indivíduos motivados. Dê a eles o ambiente e o suporte e confie que farão o trabalho;
6. O método mais eficiente e efetivo de transmitir informações entre/para um time de desenvolvimento é por meio de uma conversa cara a cara;
7. Software funcional é a medida primária de progresso;
8. Processos ágeis promovem um desenvolvimento sustentável. Patrocinadores, desenvolvedores e usuários devem ser capazes de manter o ritmo constante;
9. Atenção contínua à excelência técnica e ao bom design aumenta a agilidade;
10. Simplicidade – a arte de maximizar a quantidade de trabalho não feito – é essencial;
11. As melhores arquiteturas, requisitos e projetos emergem de equipes auto-organizadas;
12. Em intervalos regulares, a equipe reflete sobre como se tornar mais efetiva, em seguida, ajusta seu comportamento de acordo com a meta.

Desde o Manifesto Ágil, a popularidade e sucesso dos processos ágeis de desenvolvimento de software se deram devido à ênfase nas equipes, entrega frequente de software, colaboração do cliente, respostas eficazes às mudanças, melhoria contínua, equipes autogeridas e avaliações internas (GILL; HENDERSON-SELLERS; NIAZI, 2018; MIRZA; DATTA, 2019; REDDY; KUMAR, 2020).

Além dos fatores apontados, a introdução de histórias de usuários na representação de necessidades dos usuários foi determinante para o sucesso dos processos ágeis de desenvolvimento de software, pois modificaram como as definições e organizações dos requisitos do sistema são especificados (MIRZA; DATTA, 2019; REDDY; KUMAR, 2020).

Ao contrário da documentação formal de análise de requisitos dos modelos tradicionais da Engenharia de Software, as histórias de usuário devem ser escritas de maneira simples e curtas, utilizando linguagem natural semiestruturada a partir da perspectiva do usuário sobre a funcionalidade do sistema de software (COHN, 2004). Além disso, ao longo do ciclo de vida do projeto, as histórias de usuário auxiliam a

compartilhar a compreensão dos objetivos e funções esperadas no sistema (CHOMA; ZAINA; BERALDO, 2016; KANNAN *et al.*, 2019).

Segundo Lucassen (2016), os times ágeis de desenvolvimento utilizam diferentes *templates* para escrever histórias de usuário. Entretanto, o modelo Connextra (COHN, 2004) é o mais utilizado pela indústria e, por este motivo, será o *template* utilizado como base para este trabalho. A estrutura original do modelo é dada como:

*"**Como um** <ator>**, eu quero** <objetivo>**, para que** <benefício>"*

O modelo possui três argumentos (COHN, 2004):

- ator: descreve um tipo de usuário do sistema que realizará uma determinada ação ou que espera que o sistema realize determinada operação;
- objetivo: detalha a ação que será executada pelo sistema em suporte ao ator;
- benefício: fornece a justificativa para a ação do ponto de vista do ator.

Exemplos de utilização do modelo Connextra (COHN, 2004) na escrita de história de usuário:

*"**Como um** usuário, **eu quero** acessar minha conta, **para que** eu possa gerenciar meu dinheiro" (GRALHA et al., 2022).*

*"**Como um** cliente, **eu quero** transferir fundos entre minhas contas vinculadas, **para que** eu possa financiar meu cartão de crédito" (AMNA; POELS, 2022).*

Atualmente as histórias de usuário são utilizadas por vários processos ágeis de desenvolvimento de software, sendo os mais populares o Kanban (ANDERSON; CARMICHAEL, 2016) e Scrum (SCHWABER; SUTHERLAND, 2020), sendo esse último o mais utilizado pela indústria (MIRZA; DATTA, 2019; REDDY; KUMAR, 2020).

2.1.1 Scrum

A concepção inicial do modelo Scrum ocorreu na indústria automobilística (TAKEUCHI; NONAKA, 1986), porém o modelo foi adaptado a várias outras áreas, dentre elas, o desenvolvimento de softwares, que define o Scrum como um modelo ágil de gerenciamento de projetos de software, tendo seus princípios consistentes com o Manifesto Ágil (PRIES; QUIGLEY, 2010; SCHWABER; BEEDLE, 2002).

O Scrum tem como objetivo orientar as atividades de desenvolvimento de sistemas em um processo de software, além de possuir algumas características como: entregas frequentes e intermediárias de funcionalidades, planejamento de mitigação de riscos ao projeto, transparência no planejamento e desenvolvimento das atividades, possibilidade dos clientes tornarem-se parte da equipe de desenvolvimento, e reuniões diárias na qual os membros do time de desenvolvimento respondem questões relacionadas às atividades e metas (PRIES; QUIGLEY, 2010).

No modelo Scrum há três perfis importantes, segundo Schwaber e Sutherland (2020): *Scrum Master, Product Owner* e *Team*. O primeiro é responsável por orientar a equipe e atuar como um facilitador para que o *Team* consiga desempenhar suas atividades da melhor maneira possível. Além disso, o *Scrum Master* é o especialista em melhores práticas Scrum, e sua missão é garantir que as práticas ágeis sejam adotadas durante todo o processo de desenvolvimento.

O segundo perfil, denominado *Product Owner*, faz a comunicação entre o cliente e o time de desenvolvimento (*Team*). É de responsabilidade do *Product Owner* ter conhecimento do mercado e estar completamente familiarizado com o negócio do cliente, pois desta maneira saberá especificar e priorizar as funcionalidades que serão implementas.

Por fim, o *Team* é a equipe de desenvolvimento a qual é responsável por modelar, implementar, testar e validar as funcionalidades elicitadas. Como não há uma figura de gerente de projeto, o *Team* é autogerenciado. A interação entre os membros da equipe deve ser constante, pois a qualidade do produto final gerado depende da integração das atividades desenvolvidas por cada um.

Além dos perfis, o modelo Scrum possui dois artefatos (SCHWABER; SUTHERLAND, 2020), o *Product Backlog* e o *Sprint Backlog*. O primeiro é caracterizado por uma lista priorizada de requisitos elicitados que serão posteriormente desenvolvidos. O segundo refere-se a lista de itens selecionados do

Product Backlog que serão implementados na próxima iteração de desenvolvimento, chamado de *Sprint*.

Para que o modelo funcione corretamente, em todas as etapas do processo de desenvolvimento há eventos que precisam ser realizados (SCHWABER; SUTHERLAND, 2020): *Sprint Planning Meeting, Daily Scrum Meeting, Sprint Review* e *Sprint Retrospective.* A Figura 1 ilustra uma visão geral do processo de gerenciamento ágil Scrum.

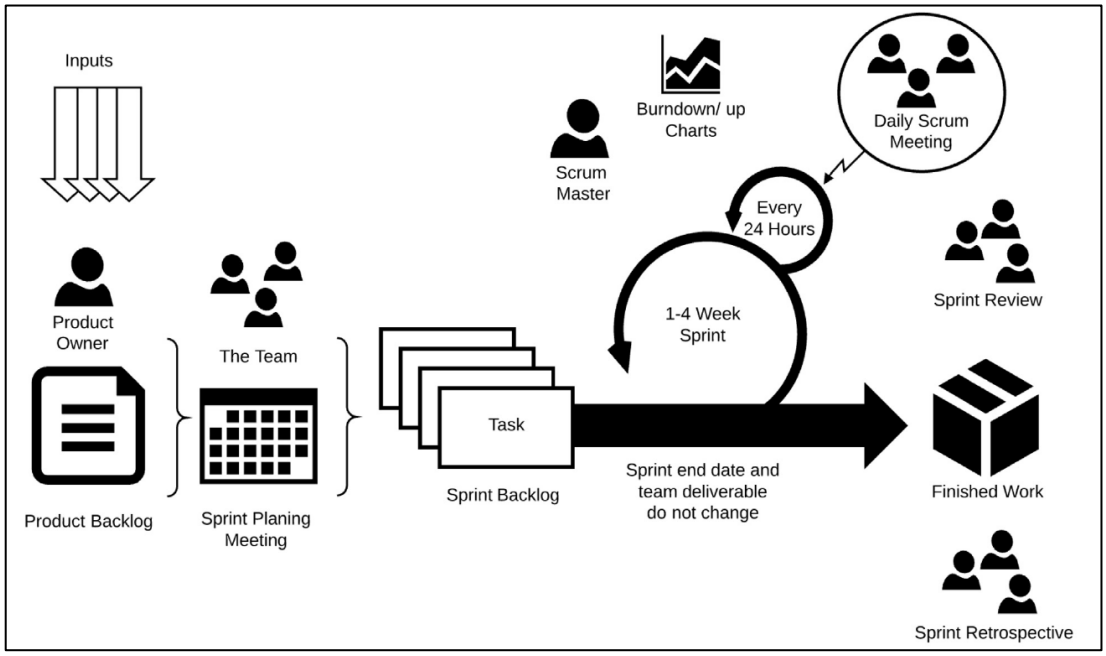

Figura 1. Processo Scrum (SCHWABER; SUTHERLAND, 2020).

O início de um novo projeto ocorre com o recebimento de contribuições, também chamadas de histórias do usuário, pelo *Product Owner*. No início do ciclo de vida de desenvolvimento, algumas destas histórias podem ser vagas, porém, conforme o processo avança, novas contribuições são realizadas e o processo de maturação destes itens ocorre naturalmente. Este processo é denominado de descoberta do produto. Ao obter um número suficiente de itens (histórias do usuário), estes são priorizados considerando os requisitos essenciais de negócio e suas dependências. A lista priorizada é ilustrada na Figura 1 pelo *Product Backlog*.

A cada novo ciclo de desenvolvimento, denominado de *Sprint*, o *Team* realiza a *Sprint Planning Meeting.* Nesta reunião ocorre a seleção dos itens a serem implementados – chamados de *Features,* na Figura 1. Esta lista de itens é chamada

de *Sprint Backlog*. Cada *Sprint* possui um período curto e limitado de trabalho que, segundo Schwaber e Sutherland (2020), pode durar de 1 a 4 semanas.

Após o início da *Sprint*, todos os dias a *Daily Scrum Meeting* é realizada com o propósito de manter cada indivíduo da equipe atualizado com o andamento das atividades dos outros membros. Este encontro possui um horário específico para iniciar e deve durar no máximo 15 minutos. Cada integrante deve permanecer em pé durante todo o tempo e responder três questões: (i) o que você fez no dia anterior? (ii) o que você está planejando fazer no dia de hoje? e (iii) há algum problema que lhe impeça de realizar seu objetivo?

Ao final de cada ciclo do *Sprint* é realizada a Reunião de Revisão do *Sprint (Sprint Review)* e a Retrospectiva do *Sprint (Sprint Retrospective).* A primeira visa discutir sobre as atividades que foram desenvolvidas no decorrer do *Sprint*, e a segunda tem o intuito de fazer os membros da equipe refletirem sobre o último *Sprint,* com um olhar crítico e, se possível, propor melhorias para futuras iterações.

Como trata-se de um processo iterativo, ao finalizar um *Sprint* se iniciará outro, até que o *Product Backlog* seja consumido e, consequentemente, o produto final atenda os critérios de aceitação do cliente (SCHWABER; SUTHERLAND, 2020).

2.1.2 Kanban

Kanban é um termo japonês que pode ser entendido como “cartão” ou “quadro indicador” (ANDERSON, 2010; SUGIMORI *et al.*, 1977) e é baseado no sistema de puxar atividades/tarefas (HUANG; KUSIAK, 1996; KIMURA; TERADA, 1981).

O método Kanban surgiu em conjunto com a manufatura Lean, desde então outras áreas o utilizam, como por exemplo, aeronáutica, saúde, varejo, recursos humanos e Engenharia de Software (DENNEHY; CONBOY, 2017; POPPENDIECK; CUSUMANO, 2012; POWER; CONBOY, 2015). Nesta última, o método Kanban foi bem recebido e, nos últimos anos, cada vez mais equipes o tem adotado. Conforme apontam os relatórios anuais “*State of Agile*”, em 2014, 31% dos entrevistados responderam utilizar o método Kanban como uma técnica ágil de desenvolvimento de software. Entretanto, nove anos depois, em 2022, a porcentagem aumentou para 56% (VERSIONONE INC., 2015, 2022).

Segundo Anderson (2010), o método Kanban visa auxiliar em vários fatores a Engenharia de Software, como por exemplo, aumentar a confiabilidade do cliente,

obter respostas satisfatórias às solicitações das mudanças, minimizar os custos e tempo de entrega do desenvolvimento de software. Para isso, são propostos cinco princípios Kanban (ANDERSON, 2010): (i) visualizar o fluxo de trabalho; (ii) limitar o trabalho em andamento; (iii) tornar as políticas de processo explícita; (iv) medir e gerenciar o fluxo; e (v) usar modelos para reconhecer oportunidades de melhoria.

O primeiro princípio, visualizar o fluxo de trabalho, menciona que à medida que a atividade avança pela organização, ela passa por diferentes estados, como por exemplo, “À Fazer”, “Em Desenvolvimento”, “Testando” e “Feito”. Comumente estes estados são organizados em colunas no quadro Kanban, conforme ilustra a Figura 2.

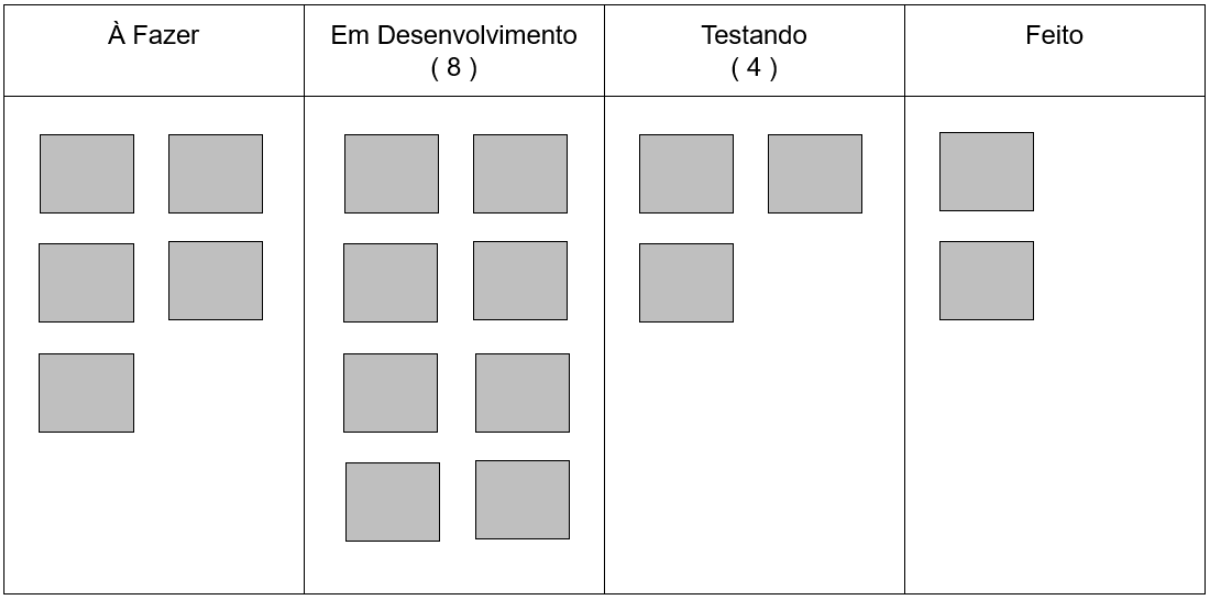

Figura 2. Exemplo de Uso do Método Kanban. Adaptado de Anderson e Carmichael (2016).

As atividades, representadas na cor cinza, são cartões físicos ou virtuais, assim, é possível que as equipes visualizem o fluxo de trabalho conforme ocorre a movimentação das atividades pela organização, pois cada cartão é fixado em uma coluna, de acordo com seu estado atual.

Para que as atividades que estão com estado “Em Desenvolvimento” ou “testando” não se acumulem e permaneçam inacabadas, é necessário estabelecer um número máximo de atividades que podem estar sendo desenvolvidas paralelamente (que podem estar fixadas na coluna). Este princípio denomina-se limitar o trabalho em andamento e é observado pelos valores 8 (oito) e 4 (quatro) nas colunas “Em Desenvolvimento” e “Testando”, respectivamente. Deste modo, a equipe terá seu foco

em poucas atividades que devem ser finalizadas para que, posteriormente, novas atividades sejam iniciadas.

Políticas explícitas, também chamadas de critérios de entrada e saída, devem ser estabelecidas para determinar quando uma atividade pode ser puxada de um estado para outro (POWER, 2014). Este princípio é denominado tornar as políticas de processo explícitas.

O princípio de medir e gerenciar o fluxo visa conhecer as etapas que uma determinada atividade deve passar até que seja concluída e o tempo gasto em cada uma das etapas. Algumas das métricas que podem ser utilizadas neste princípio: (i) *lead time*, permite analisar o tempo total do ciclo de uma atividade, desde sua criação até sua conclusão; (ii) *cycle time*, semelhante ao lead time, porém no *cycle time* o início é considerado no momento que a atividade passa para o estado “Em Desenvolvimento”; (iii) *throughput*, mensura a quantidade de atividades concluídas em um determinado período de tempo; e (iv) *flow efficiency*, que auxilia na redução do tempo não produtivo no fluxo de uma atividade, como por exemplo, quando uma determinada atividade não está efetivamente “Em Desenvolvimento”, mas à espera da resolução de alguma pendência.

Por fim, após obter o conhecimento de todo o fluxo de trabalho, bem como seus possíveis problemas, é necessário evoluí-lo. Para isso, deve-se engajar a equipe e promover pequenas alterações no processo a fim de não causar resistência à mudança.

2.2 Princípios da Privacidade

O conceito de privacidade foi definido em 1890 por Warren e Brandeis (1890) como o “direito de ser deixado em paz”. Anos depois, Westin (1967) escreveu que a privacidade é “a capacidade do indivíduo de controlar os termos sob os quais as informações pessoais são adquiridas e utilizadas”, significando que um indivíduo deve possuir o controle sobre como seus dados pessoais são coletados, caso contrário, resultará na invasão da privacidade, uso indevido e/ou não autorizado e outras violações de direitos fundamentais. Em 1975, Altman (1975) descreveu a privacidade como “o controle seletivo de acesso a si mesmo”.

Em resposta ao uso crescente de sistemas automatizados de informações contendo dados pessoais, o Comitê Consultivo do Secretário dos Estados Unidos em

Sistemas Automatizados de Dados Pessoais, em 1973, propôs um código de práticas justas a partir de um conjunto de princípios (FIPPs, em inglês *Fair Information Practice Principles),* para uso de dados pessoais em sistemas automatizados (SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, 1973).

À medida em que os anos se passaram, surgiram outras leis, regulamentos e diretrizes de privacidade, principalmente no continente europeu e asiático. Por exemplo, as Diretrizes da OECD (em inglês *Organisation for Economic Cooperation and Development*), desenvolvidas em 1980 pela Organização para a Cooperação e Desenvolvimento Econômico, e a organização para a Cooperação Econômica da Ásia-Pacífico (APEC, em inglês *Asia-Pacific Economic Cooperation*), criada em 1989, em resposta à crescente interdependência das economias da região Ásia-Pacífico.

Ao longo dos anos, a indústria percebeu que quanto maior o nível de privacidade fornecido ao titular dos dados, menos inovações em seus produtos eram possíveis. Por outro lado, quanto mais inovações eram feitas, menor era o nível de privacidade fornecido. Esse dilema é conhecido como soma zero (ALSHAMMARI, 2019). Neste contexto, a abordagem *Privacy by Design* (PbD) (CAVOUKIAN, 2009a) foi concebida com o intuito de equilibrar a relação inovação e proteção de dados pessoais em uma relação de soma positiva, para que não seja necessário sacrificar funcionalidades do sistema ao incorporar a proteção de dados pessoais.

Ressalta-se que na literatura, o termo "Privacidade de Dados Pessoais" era comumente aceito e aplicado em todas as situações. Entretanto, em meados da última década, com a discussão e implantação de novas leis e regulamentos, como o *General Data Protection Regulation (GDPR)* (EU, 2016), da União Europeia, e a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a), atualmente em vigor no Brasil, o termo "Proteção de Dados Pessoais" passou a ser entendido como um direito fundamental a ser garantido por meio de medidas legais, técnicas e organizacionais adotadas para garantir a proteção dos dados pessoais contra acessos não autorizados, perda, destruição ou danos, o que inclui a implementação de controles de segurança, políticas de acesso, criptografia, *backups* regulares e outras práticas para proteger os dados contra ameaças internas e externas.

2.2.1 Privacy by Design

Em sua concepção, o *Privacy by Design* (PbD) possui o intuito de envolver os Princípios da Prática de Informação Justa (FIPP, em inglês *Fair Information Practice Principles*), tornando-se parte integrante das prioridades organizacionais, objetivos de projeto, processos de design, desenvolvimento, operações e gerenciamento. Em um primeiro momento, a principal área de aplicação era em Tecnologia da Informação (TI), porém, posteriormente seu domínio estendeu-se para outras áreas, como práticas de negócios e projetos físicos, sendo assim, uma abordagem abrangente e eficaz (CAVOUKIAN, 2009a, 2009b).

Segundo Cavoukian *et al.* (2014), o PbD deve ser utilizado para integrar a privacidade e a proteção de dados pessoais durante todas as fases do projeto, desde os estágios iniciais até sua concepção, passando pelos processos organizacionais, arquiteturas de rede e aprimoramento de sistemas de governança. Além disso, o PbD presume que não há como atingir níveis satisfatórios de proteção da privacidade de dados pessoais apenas cumprindo padrões legais. Ao contrário, a garantia de privacidade deve ser um “modo padrão de operação” (CAVOUKIAN, 2009a).

Ao todo, PbD contém 7 (sete) princípios fundamentais capazes de fornecer um *framework* abrangente para integrar os requisitos de privacidade de maneira proativa e eficiente nas fases iniciais do processo de design (CAVOUKIAN, 2009a): (i) *Proactive not Reactive; Preventative not Remedial;* (ii) *Privacy as the Default;* (iii) *Privacy Embedded into Design;* (iv) *Full Functionality – Positive-Sum, not Zero-Sum;* (v) *End-to-End Security – Lifecycle Protection;* (vi) *Visibility and Transparency;* e (vii) *Respect for User Privacy*.

Estes princípios contribuíram para que, em outubro de 2010, na *32nd International Conference of Data Protection and Privacy Commissioners*, que ocorreu na cidade de Jerusalém, o PbD fosse unanimemente adotada como padrão internacional de privacidade (CAVOUKIAN, 2012b) e, nos anos seguintes, tivesse influências em legislações de vários países, como na *General Data Protection Regulation* (EU, 2016), da União Europeia e a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018a), atualmente em vigor no Brasil.

As subseções a seguir abordam os 7 (sete) princípios do *Privacy by Desing* definidos por Cavoukian (2009a).

2.2.1.1 Proativo não Reativo; Prevenir não Remediar

Cavoukian (2009a) descreve o princípio Proativo não Reativo; Prevenir não Remediar, como:

> A abordagem *Privacy by Design* é caracterizada por medidas proativas, em vez de reativas. Ele antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. O PbD não espera que os riscos de privacidade se materializem, nem oferece soluções para resolver infrações de privacidade uma vez que ocorram - tem como objetivo evitar que ocorram. Resumindo, o *Privacy by Design* vem antes do fato, não depois. (p. 2, tradução livre)[13]

Para respeitar este princípio, deve-se adotar um conjunto definido de objetivos e requisitos de privacidade desde o início do projeto, como por exemplo, desvinculação, transparência, limitação de coleta e uso, qualidade de dados, especificação de propósito, entre outros. Isto proporciona a possibilidade de avaliar, revisar e corrigir as soluções de privacidade, antes mesmo que sejam implementadas e tornem-se problemas mais complexos, pois quanto mais tardia implementação/correção dos riscos à privacidade, mais difíceis e caros de corrigi-los.

Considerar os detalhes técnicos do ciclo de vida dos dados de modo proativo também faz parte desde princípio. Neste caso, deve-se planejar com antecedência como os dados serão inseridos e utilizados pelo sistema, bem como a sua anonimização.

2.2.1.2 Privacidade por Padrão

O princípio da privacidade por padrão é definido por Cavoukian (2009a) como:

> Todos nós podemos ter certeza de uma coisa - as regras como padrão! O *Privacy by Design* visa fornecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. Se um indivíduo não fizer nada, sua privacidade ainda permanecerá intacta. Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade - isso é integrado ao sistema, por padrão. (p. 2, tradução livre)[14]

---

[13] Proactive not Reactive; Preventative not Remedial – The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after (CAVOUKIAN, 2009a, p. 2).

[14] Privacy as the Default – We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still

A implementação deste princípio garante ao titular a proteção de seus dados sem qualquer ação necessária por parte dele. Além disso, possibilita ao titular o controle da quantidade e qualidade de dados que deseja divulgar.

Um modo de implementar este princípio é por meio da minimização de dados. Neste caso, o sistema solicita apenas uma quantidade mínima necessária de dados ao titular para que consiga fazer uso de funcionalidades essenciais da aplicação. Caso o usuário necessite de funcionalidades opcionais, o sistema pode solicitar informações adicionais, sempre preservando a privacidade dos dados (BIER *et al.*, 2012).

Porém, a coleta de dados, por mínima que seja, deve estar associada a especificação de finalidade, pois é necessário comunicar ao titular dos dados para quais fins os dados serão tratados. Cavoukian (2009a) menciona que quando a necessidade ou o uso de dados pessoais não estiver bem especificado, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Isto é, as configurações padrão devem ser as mais protetoras da privacidade. Por outro lado, a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a) estabelece que cada dado coletado precisa ter uma finalidade, um tempo de retenção e uma hipótese de tratamento especificada e informada.

2.2.1.3 Privacidade Incorporada no Design

A Privacidade Incorporada no Design é descrita por Cavoukian (2009a) como:

> *Privacy by Design* está embarcada no projeto e na arquitetura dos sistemas de TI e nas práticas de negócios. Não é inserido como um *add-on* em fases tardias de desenvolvimento. O resultado é que a privacidade se torna um componente essencial da funcionalidade central que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade. (p. 3, tradução livre)[15]

Para Cavoukian, a privacidade deve, de maneira holística, integrativa e criativa, ser uma característica central e incorporada às tecnologias, operações e arquiteturas. Holística para que considere contextos adicionais e mais amplos. Integrativa para que

---

remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default (CAVOUKIAN, 2009a, p. 2).

[15] Privacy Embedded into Design Privacy – Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality (CAVOUKIAN, 2009a, p. 3).

consulte todos os *stakeholders* e seus interesses. E, por fim, criativa, pois em determinados casos, incorporar a privacidade significa reinventar escolhas existentes porque as alternativas podem não ser mais aceitáveis.

Além disso, o processo de design deve identificar, desde seu início, os riscos que ameaçam a privacidade dos titulares de dados, conseguindo assim, definir estratégias de mitigações também nas primeiras etapas do projeto e minimizando as chances de fazer trabalhos desnecessários no futuro (CAVOUKIAN, 2009a).

2.2.1.4 Funcionalidade Total – Soma Positiva, não Soma Zero

Funcionalidade Total – Soma Positiva, não Soma Zero, é apresentada por Cavoukian (2009a) como:

> O *Privacy by Design* visa acomodar todos os interesses e objetivos legítimos de uma forma de soma positiva e "ganha-ganha", não por meio de uma abordagem datada e de soma zero, pela qual compensações desnecessárias são realizadas. O *Privacy by Design* evita a pretensão de falsas dicotomias, como privacidade x segurança, demonstrando que é possível, e muito mais desejável, ter ambas. (p. 3, tradução livre)[16]

É comum posicionar a proteção de dados como soma zero, pois compete com outros interesses, objetivos e capacidades técnicas de um determinado domínio. Porém, o PbD vai contra este posicionamento. Deve-se, além de cumprir os requisitos relacionados à privacidade, como por exemplo, anonimização, confidenciabilidade, transparência, entre outros, também se deve satisfazer os objetivos legítimos dos usuários. Desta maneira, ao incorporar proteção de dados em uma determinada tecnologia, processo ou sistema, esta tarefa deve ser realizada de modo que não prejudique a sua funcionalidade total.

Finalmente, os objetivos do ponto de vista do desenvolvedor devem ser documentados, funções desejadas precisam ser articuladas, métricas acordadas e aplicadas, e os conflitos de escolhas solucionados para que seja possível encontrar uma solução em que ambas as partes se beneficiem sem fazer concessões indevidas (CAVOUKIAN, 2009a).

---

[16] Full Functionality – Positive-Sum, not Zero-Sum Privacy – Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win- win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both (CAVOUKIAN, 2009a, p. 3).

2.2.1.5 Segurança da Informação de Ponta a Ponta – Proteção no Ciclo de Vida

Cavoukian (2009a) descreve o princípio de Segurança da Informação de Ponta a Ponta – Proteção no Ciclo de Vida, como:

> O *Privacy by Design*, tendo sido incorporada ao sistema antes do primeiro elemento de informação ser coletado, se estende com segurança por todo o ciclo de vida dos dados envolvidos - fortes medidas de segurança são essenciais para a privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e, em seguida, destruídos com segurança no final do processo, em tempo hábil. Assim, o *Privacy by Design* garante do início ao fim, o gerenciamento seguro do ciclo de vida das informações, de ponta a ponta. (p. 4, tradução livre)[17]

Os dados pessoais devem ser protegidos continuamente em todo o domínio e ciclo de vida dos dados. Não pode, em hipótese alguma, haver falhas na proteção de dados pessoais e, por isso, a segurança possui relevância neste princípio. Segundo Cavoukian (2009a), não há como obter proteção de dados em um ambiente digital em que a segurança da informação é precária.

Para Cavoukian, as entidades devem assumir a responsabilidade pela segurança dos dados garantindo a confidencialidade, integridade e disponibilidade ao longo de todo o ciclo de vida dos dados pessoais, incluindo métodos seguros de controle de acesso, criptografia e eliminação dos dados após o término de seu tratamento.

2.2.1.6 Visibilidade e Transparência

O princípio de Visibilidade e Transparência é definido por Cavoukian (2009a) como:

> O *Privacy by Design* visa garantir a todos *stakeholders* que, seja qual for a prática comercial ou tecnologia envolvida, ela está, de fato, operando de acordo com as promessas e objetivos declarados, sujeita a verificação independente. Seus componentes e operações permanecem visíveis e

[17] End-to-End Security – Lifecycle Protection – Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end (CAVOUKIAN, 2009a, p. 4).

> transparentes, tanto para usuários quanto para provedores. Lembre-se, confie, mas verifique! (p. 4, tradução livre)[18]

Cavoukian (2009a) cita que a manutenção do controle sobre o tratamento de dados pessoais deve ser realizado pelo titular, e para isto, é primordial que ele tenha ciência sobre a existência de tratamento a partir de seus dados pessoais. Neste caso, os agentes de tratamento de dados devem ter uma política de transparência e informar ao titular sobre a utilização dos dados. Entretanto, a LGPD (BRASIL, 2018a) estabelece que o tratamento dos dados pessoais é realizado pelo controlador, mediante umas das hipóteses de tratamento estabelecido no artigo 7º da lei referida.

Tanto o tratamento quanto a comunicação com os titulares dos dados, devem ocorrer por meio de interfaces intuitivas. Tecnologias podem aumentar a transparência e ajudar na comunicação das atividades de tratamento em diversos níveis de granularidade – quanto maior o detalhamento dos dados pessoais, mais fina é a granularidade; quanto menor o detalhamento dos dados pessoais (sumarização dos dados), mais grossa é a granularidade (WANG, 2003) – além de capacitar e auxiliar os titulares a controlar quais são as informações pessoais que deseja compartilhar, bem como consentir com o tratamento dos dados pessoais (DANEZIS *et al.*, 2015).

2.2.1.7 Respeito pela Privacidade do Usuário

O Respeito pela Privacidade do Usuário é apresentado por Cavoukian (2009a) como:

> Acima de tudo, *Privacy by Design* exige que os arquitetos e agentes de tratamento mantenham os interesses do indivíduo em primeiro lugar, oferecendo medidas como fortes padrões de privacidade, aviso apropriado e opções amigáveis ao usuário. Mantenha-se centrado no usuário! (p. 5, tradução livre)[19]

Considerar os interesses e necessidades dos usuários ao realizar um projeto favorecem a obtenção dos melhores resultados do PbD. Isso se dá pelo fato destes obterem o maior interesse investido no gerenciamento de seus próprios dados

[18] Visibility and Transparency – Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify! (CAVOUKIAN, 2009a, p. 4).
[19] Respect for User Privacy – Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric! (CAVOUKIAN, 2009a, p. 5)

pessoais. Para Cavoukian (2009a), a verificação mais eficaz contra violações de privacidade se dá pela capacitação dos titulares de dados ao desempenhar um papel ativo na gestão de suas informações.

Apesar do PbD e seus 7 (sete) princípios visarem auxiliar a implantação de requisitos de privacidade durante todo o ciclo de desenvolvimento do software, ser adotada como padrão internacional de privacidade (CAVOUKIAN, 2012b) e citada como prática a ser seguida, tanto no *General Data Protection Regulation* (EU, 2016) quanto na Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018a), o PbD é criticado pela falta de diretrizes operacionais e ferramentas que auxiliem os desenvolvedores de software à aplicar na prática os 7 (sete) princípios (BALDASSARRE *et al.*, 2020; BU *et al.*, 2020; VESELI *et al.*, 2019).

Na tentativa de aproximar os princípios do PbD à Engenharia de Software, outros autores estabeleceram catálogos e/ou práticas, por exemplo, as Estratégias de Privacidade de Hoepman (HOEPMAN, 2014), descrita na Seção 2.2.2.

2.2.2 Hoepman Privacy Design Strategies

Com o intuito de auxiliar os engenheiros de software no cumprimento dos requisitos de privacidade a partir dos estágios iniciais do processo de design, Hoepman (2014) propôs um conjunto de 8 (oito) estratégias que descrevem abordagens fundamentais para alcançar um determinado objetivo e, consequentemente, níveis satisfatórios de proteção de privacidade.

A construção das *Privacy Design Strategies* (HOEPMAN, 2014), tratadas neste trabalho como Estratégias de Privacidade de Hoepman, são derivadas de princípios existentes de privacidade e leis de proteção de dados pessoais, e são divididas em duas categorias (COLESKY; HOEPMAN; HILLEN, 2016): Estratégias Orientadas a Dados e Estratégias Orientadas a Processos. Enquanto a primeira refere-se ao processamento de dados amigável à proteção de dados pessoais e possui as estratégias: (i) *Minimise*; (ii) *Hide*; (iii) *Separate*; e (iv) *Aggregate/Abstract*; a segunda destaca os processos que envolvem o tratamento responsável de dados pessoais. Nela encontram-se as estratégias: (v) *Inform*; (vi) *Control*; (vii) *Enforce*; e (viii) *Demonstrate* (HOEPMAN, 2014).

Minimise é a estratégia de design de proteção de dados mais básica, pois a quantidade de dados pessoais coletados e tratados deve ser mínima até atingir os

objetivos de funcionalidade. A decisão desta coleta pode ser realizada ainda em projeto ou em tempo de execução, e pode ocorrer de duas maneiras: optar por não coletar nenhum dado do titular ou optar por coletar apenas um conjunto limitado de dados do titular. Gürses *et al.* (2011) argumenta que ao garantir que dados desnecessários não sejam coletados em um determinado sistema, uma possível violação deste sistema causará um impacto limitado na privacidade do titular dos dados.

A estratégia de ocultação, denominada *Hide*, afirma que quaisquer dados pessoais e seus inter-relacionamentos devem ser ocultados da vista de todos, pois uma vez que estes não permanecem facilmente acessíveis, não poderão ser violados. O objetivo desta estratégia é garantir a confidencialidade[20] e desvinculação[21], garantindo assim que dois eventos distintos não possam ser correlacionados (PFITZMANN; HANSEN, 2010). Algumas medidas utilizadas nestes contextos são a dissociação, criptografia e ofuscação de dados pessoais.

Para evitar reunir informações suficientes sobre um determinado indivíduo, os dados pessoais devem ser distribuídos**,** tanto em seu armazenamento quanto em sua operação. Esta estratégia é denominada *Separate*. Este princípio exige processamento distribuído ao invés de centralizado. Armazenamento em banco de dados distintos não vinculados entre si se não for necessário e, quando possível, dividir as tabelas responsáveis pelo armazenamento dos dados no banco de dados.

A estratégia *Aggregate*, também conhecida como *Abstract*, menciona que os dados pessoais devem ser tratados no nível mais alto de abstração possível, porém ainda úteis para a operação. O objetivo desta estratégia é deixar o dado em um nível de alta granularidade ao ponto de restringir a quantidade de detalhes nos dados pessoais. Assim, quando os dados estiverem satisfatoriamente granulados e o tamanho do grupo a ser analisado é suficientemente numeroso, não há como atribuir um determinado dado à uma pessoa específica.

Os requisitos de transparência para com o titular dos dados são mencionados na estratégia *Inform*. Esta estratégia estabelece que informações relacionadas ao

---

[20] Confidencialidade: ações tomadas para assegurar que informações **confidenciais** e críticas não sejam roubadas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas.

[21] Desvinculação: Desobrigação; ação de se desfazer de um vínculo jurídico; de tornar algo alienável, transferível.

tratamento dos dados, manutenções, políticas, explicações gerais são relacionadas a esta estratégia, como por exemplo, notificações do que é armazenado, operado ou disseminado, como os dados estão protegidos, quem possui acesso e quando serão destruídos. Além disso, quaisquer alterações e/ou violações devem ser imediatamente comunicadas ao titular.

Em complemento a estratégia *Inform,* a estratégia *Control* fornece meios aos titulares dos dados realizarem o consentimento informado, além de obter o controle de seus dados, como coleta, armazenamento, operação e disseminação, recuperação e modificação dos dados. Pois sem estes meios, pouco adianta informá-lo sobre a coleta ou uso de deus dados. A situação inversa também é válida, sem as informações completas e corretas, não há por que solicitar ao titular o seu consentimento.

A estratégia *Enforce* defende a criação, aplicação e cumprimento de uma política de privacidade relativos ao armazenamento, coleta, retenção, compartilhamento, alterações, violações ou operações de dados pessoais, antes, durante e após o desenvolvimento do sistema. Para isso, são necessárias avaliações periódicas e atualizações quando ocorrerem alterações na legislação.

Semelhante a estratégia *Enforce,* a estratégia *Demonstrate,* além de seguir uma política de privacidade, o controlador de dados precisa demonstrar explicitamente como a política de privacidade é efetivamente implementada em um sistema de Tecnologia da Informação, que pode ocorrer por meio de auditorias, registros e relatórios.

2.2.3 ISO/IEC 29100:2011

Em 2011, a Organização Internacional de Padronização (ISO, em inglês *International Organization for Standardization*) em conjunto com a Comissão Eletrotécnica Internacional (IEC, em inglês *International Electrotechnical Commission*), publicaram um *framework* universal de privacidade, denominado ISO/IEC 29100:2011, contendo onze princípios com foco na implementação de sistemas de Tecnologia da Informação (ISO/IEC 29100, 2011), a saber:

- ***Consent and choice:*** o princípio de consentimento e escolha possibilita que o titular dos dados dê seu consentimento ao processamento de seus dados pessoais, chamados na ISO/IEC 29100:2011, de Informações de Identificação Pessoal (PII, em inglês *Personally Identifiable Information*).

Este consentimento deve estar em conformidade com a política de privacidade fornecida, sendo possível o titular optar pela recusa.

- ***Purpose legitimacy and specification:*** as organizações que efetuam as coletas de dados devem informar aos potenciais usuários sobre como seus dados pessoais serão gerenciados. Para isso, deve-se usar uma linguagem clara, objetiva e não ambígua. A finalidade do processamento dos dados deve estar em conformidade com os regulamentos e legislações e o titular dos dados deve compreender o propósito da coleta antes que seja efetuada pelo sistema.
- ***Collection limitation:*** estabelece que as organizações devem limitar a coleta de informações de identificação pessoal. Apenas dados necessários para atender um determinado propósito devem ser adquiridos, sendo necessário documentar e justificar o tipo de dado pessoal coletado.
- ***Data minimization:*** as organizações devem minimizar o processamento de informações de identificação pessoal. Há diversas maneiras de contemplar este princípio, restringir o acesso de determinados dados a apenas indivíduos que necessitam, abstrair os dados a fim de reduzir/impossibilitar a identificação e a observação do comportamento do titular, são exemplos. Por fim, quando as informações não são mais úteis, elas devem ser descartadas e/ou excluídas.
- ***Use, retention and disclosure limitation:*** os propósitos de uso/processamento, retenção e divulgação das informações de identificação pessoal devem ser limitados, explícitos e legítimos, e, ao atingir o objetivo determinado, devem ser destruídos ou tornados anônimos.
- ***Accuracy and quality:*** para que seja possível às organizações utilizarem as informações de identificações pessoais, estas necessitam ser precisas, completas e relevantes. Por este motivo, é importante que as organizações estabeleçam procedimentos de coleta e validação de dados, além de mecanismos de controle que assegurem, periodicamente, a qualidade das informações.

- ***Openness, transparency and notice:*** informações sobre acessos, correções e remoções de informações devem ser fornecidas aos titulares dos dados de maneira clara, objetiva e de fácil acesso, bem como as políticas, procedimentos e práticas com relação ao processamento de seus dados pessoais. Ao alterar as práticas e políticas de privacidade os titulares dos dados devem ser imediatamente notificados.
- ***Individual participation and access:*** os titulares dos dados devem ser capazes de, por meio de procedimentos simples, rápidos e eficientes, acessar, revisar, alterar e remover seus dados pessoais.
- ***Accountability:*** é de responsabilidade da organização documentar, comunicar políticas e práticas de privacidade, fornecer treinamento adequado relacionado à privacidade, e informar a todos os interessados quanto a eventuais danos e as medidas tomadas a minimizá-lo. Deve haver na organização um profissional responsável pelos assuntos referentes à privacidade.
- ***Information security:*** a organização deve ser capaz de garantir a integridade, confidencialidade e disponibilidade das informações de identificação pessoal e protegê-las contra os riscos de segurança em todo o ciclo de vida. Para isso, é necessário que os riscos sejam tratados, revisões periódicas precisam ser realizadas e o acesso à determinada informação deve ser limitado a apenas aos indivíduos que a necessitem.
- ***Privacy compliance:*** é necessário que a organização cumpra as legislações, políticas e procedimentos de privacidade, além de realizar auditorias internas e externas com o intuito de verificar se o processamento das informações de identificação pessoal atende aos requisitos de privacidade de dados. Por fim, é necessário desenvolver e manter avaliações de risco à privacidade a fim de avaliar programas e serviços que envolvam dados pessoais.

Os onze princípios do *framework* ISO/IEC 29100:2011, derivaram de outros padrões internacionais, como por exemplo, *Fair Information Practice Principles*

(FIPPs) e *OECD Privacy Framework Privacy Principles*, e podem auxiliar o projeto, desenvolvimento e implementação de políticas e controle de privacidade nas organizações de TI, além de aprimorar os padrões de segurança existentes sempre que houver o processamento de informações de identificação pessoal (VAIDYA; MOUFTAH, 2018).

Porém, deve-se ressaltar que a maneira como as organizações de TI processam as informações que identificam os titulares dos dados, bem como as leis e regulamentações aplicáveis a essas organizações, afeta diretamente como é aplicado cada princípio da ISO/IEC 29100:2011 (MORALES-TRUJILLO *et al.*, 2019).

2.2.4 Padrões de Privacidade

Segundo Colesky *et al.* (2016), os padrões de privacidade fornecem o conhecimento coletado de especialistas de maneira estruturada, documentada e reutilizável, além de contribuírem na construção de um sistema de informação seguro. As soluções oferecidas para a utilização desses padrões de privacidade envolvem o detalhamento dos ativos de informação e o nível de criticidade desses ativos, incluindo os detalhes de implantação em um ambiente real, levando em consideração a arquitetura e as tecnologias que devem ser utilizadas (MORAL-GARCÍA *et al.*, 2011).

Portanto, os padrões de privacidade suportam a documentação de soluções comuns para problemas de privacidade e podem melhorar a maneira como os sistemas podem ser desenvolvidos, descrevendo classes, colaborações entre objetos e seus propósitos, e ajudar os designers a identificar e resolver questões relacionadas à privacidade e proteção de dados pessoais.

Vários tipos de padrões de privacidade foram propostos, tais como: padrões de privacidade para computação ubíqua (CHUNG *et al.*, 2004), padrões de privacidade para interação (ROMANOSKY *et al.*, 2006), padrões de projeto para desenvolvimento de tecnologias de aprimoramento a privacidade (*Privacy-Enhancing Technologies* - PET) (HAFIZ, 2006), padrões de processos (KALLONIATIS; KAVAKLI; GRITZALIS, 2008), padrões para a criação de políticas de privacidade (LOBATO; FERNANDEZ; ZORZO, 2009), padrões de interface de usuário para PET (GRAF *et al.*, 2010), padrões de árvore de ameaças (DENG *et al.*, 2011), e padrões de requisitos para aplicações em sistemas operacionais móveis (XUAN; WANG; LI, 2014).

Com o intuito de reunir os padrões de privacidade propostos, pesquisadores da Universidade da Califórnia mantêm um catálogo contendo, atualmente, 72 (setenta e dois) padrões de privacidade organizados em categorias. Cada padrão é estruturado de acordo com as seguintes características (MORAL-GARCÍA *et al.*, 2011; UC BERKELEY SCHOOL OF INFORMATION, 2024):

- Nome: representa o problema abordado;
- Contexto: contém uma descrição genérica da configuração e especifica as condições sob as quais o padrão de privacidade deve ser aplicado;
- Problema: apresenta a situação que levou à necessidade de aplicar mecanismos de privacidade e obter uma solução;
- Solução: descreve a solução com base no cenário e no problema considerado.

2.3 Considerações sobre o Capítulo

Neste capítulo foram apresentados os conceitos fundamentais para o desenvolvimento desta pesquisa. A Seção 2.1 apresentou como surgiram os processos de software e quais problemas enfrentaram com o passar dos anos até sua evolução para os processos ágeis de desenvolvimento de software, ocorrido no ano de 2001, com o Manifesto Ágil. Desde então, inúmeros processos ágeis de desenvolvimento foram criados, porém, esta seção abordou os mais utilizados da atualidade (MIRZA; DATTA, 2019; REDDY; KUMAR, 2020): Scrum e Kanban. Cada processo ágil de desenvolvimento de software foi descrito considerando seus valores, princípios, atividades e perfis que o compõem, bem como suas vantagens e desvantagens em relação a outros modelos de processos.

A Seção 2.2 abordou os principais princípios de privacidade para este projeto de pesquisa. A Subseção 2.2.1 apresentou o *Privacy by Design* (PbD) e seus 7 (sete) princípios fundamentais: (i) *Proactive not Reactive; Preventative not Remedial;* (ii) *Privacy as the Default;* (iii) *Privacy Embedded into Design;* (iv) *Full Functionality – Positive-Sum, not Zero-Sum;* (v) *End-to-End Security – Lifecycle Protection;* (vi) *Visibility and Transparency;* e (vii) *Respect for User Privacy*.

Na Subseção 2.2.2 foram descritas as estratégias de privacidade de Hoepman: (i) *Minimise*; (ii) *Hide*; (iii) *Separate*; e (iv) *Aggregate/Abstract*; a segunda destaca os

processos que envolvem o tratamento responsável de dados pessoais. Nela encontram-se as estratégias: (v) *Inform*; (vi) *Control*; (vii) *Enforce*; e (viii) *Demonstrate.*

A Seção 2.2.3 discorreu sobre os onze princípios do *framework* universal de privacidade ISO/IEC 29100:2011: (i) *Consent and choice;* (ii) *Purpose legitimacy and specification;* (iii) *Collection limitation;* (iv) *Data minimization;* (v) *Use, retention and disclosure limitation;* (vi) *Accuracy and quality;* (vii) *Openness, transparency and notice;* (viii) *Individual participation and access;* (ix) *Accountability;* (x) *Information security;* e (xi) *Privacy compliance*.

Por fim, na Subseção 2.2.4 foram descritos os 72 (setenta e dois) padrões de privacidade catalogados pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024). Os padrões são estruturados de acordo com seu nome, contexto, problema e solução, e respaldam a elaboração de soluções convencionais para desafios na área de proteção de dados, podendo aprimorar a abordagem do desenvolvimento de softwares ao descrever classes, interações entre objetos e seus propósitos. Isso auxilia os designers na identificação e resolução de questões ligadas à proteção de dados pessoais.

CAPÍTULO 3 - ESTRUTURAÇÃO DA PESQUISA

Este capítulo apresenta as etapas para a condução da pesquisa. De acordo com Collis e Hussey (2009), uma pesquisa pode ser classificada de acordo com seu objetivo em: pesquisa exploratória, descritiva ou avaliativa. Segundo Wohlin e Aurum (2015) a pesquisa exploratória é aplicada quando não há muita informação disponível na área do tópico e a pesquisa tem como objetivo reunir alguns *insights* sobre o problema. O objetivo é explorar a área e fornecer informações para uma investigação mais aprofundada. A investigação exploratória pode ser tanto qualitativa como quantitativa.

Considerando os objetivos da pesquisa, descritos no Capítulo 1, pode-se caracterizá-la como uma pesquisa exploratória, uma vez que visa identificar como apoiar equipes de desenvolvimento de software na implementação dos princípios do *Privacy by Design*. A Seção 3.1 apresenta a estratégia de pesquisa adotada no desenvolvimento desta tese.

3.1 Estratégia de Pesquisa

Esta pesquisa utiliza o método de pesquisa *Design Science Research Methodology* (DSRM) (PEFFERS *et al.*, 2007), que possui seis atividades principais descritas nas respectivas seções:

- Identificação do Problema e Motivação (Subseção 3.1.1);
- Definição dos Objetivos para uma Solução (Subseção 3.1.2);
- Projeto e Desenvolvimento (Subseção 3.1.3);
- Demonstração (Subseção 3.1.4);
- Avaliação (Subseção 3.1.5); e
- Comunicação (Subseção 3.1.6).

A Figura 3 ilustra o método de pesquisa adotado. Cada atividade (em azul) inclui um conjunto de etapas (em cinza).

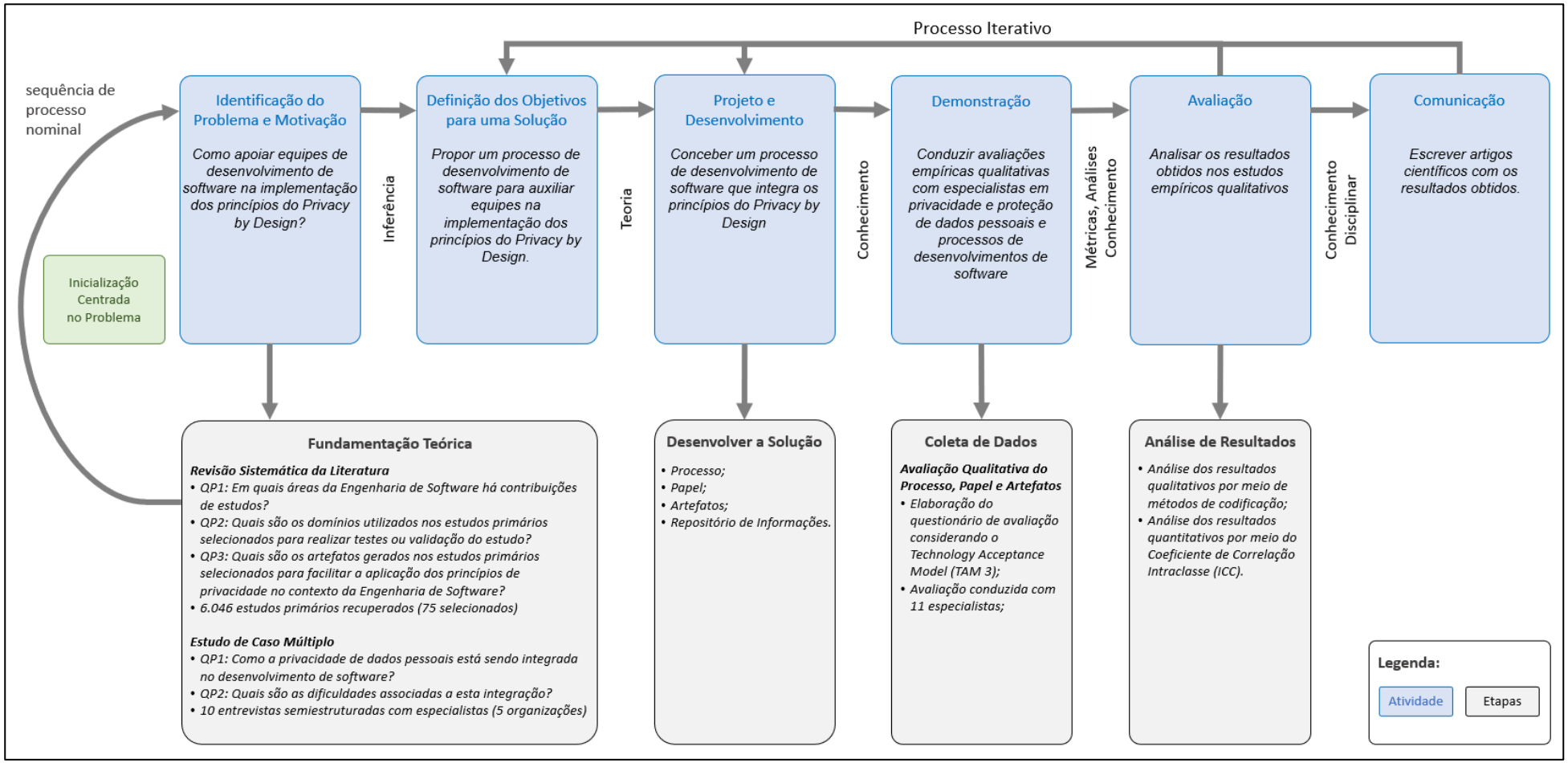

Figura 3. Método de Pesquisa. Adaptado de Peffers (2007).

3.1.1 Identificação do Problema e Motivação

Por meio de uma análise exploratória realizou-se a identificação de trabalhos referentes a abordagem *Privacy by Design* e Engenharia de Software. Alguns trabalhos que fomentaram esta pesquisa foram Senatah *et al.* (2017), Notario *et al.* (2015), Kost *et al.* (2011), Morales-Trujillo *et al.* (2019), entre outros.

Devido à necessidade de um maior aprofundamento do conhecimento das pesquisas realizas em *Privacy by Design* na área de Engenharia de Software, realizou-se uma Revisão Sistemática de Literatura (RSL) (ANDRADE *et al.*, 2022), a qual foi conduzida seguindo as diretrizes propostas por Kitchenham e Charters (2007) e Petersen *et al.* (2015), e é apresentada em detalhes no Capítulo 4.

Após a conclusão da RSL, foram realizados estudos de casos (ANDRADE *et al.*, 2023) com organizações de desenvolvimento de software com o intuito de compreender como a privacidade de dados pessoais está sendo integrada no processo de desenvolvimento de software. A adoção de estudo de caso como estratégia desta etapa da pesquisa deu-se pelo fato de ser um método adequado na condução de pesquisas de natureza descritiva e é abordado em detalhes no Capítulo 5.

3.1.2 Definição dos Objetivos para uma Solução

Baseado na RSL realizada, verificou-se a dificuldade de implementar na prática os conceitos do *Privacy by Design* na Engenharia de Software. Isso se dá pelo alto nível de abstração de seus princípios que não deixam explícito como implementá-los na prática em um projeto de desenvolvimento de software, sendo necessário a criação de processos que guiem engenheiros de softwares a fazê-lo, como apontam os trabalhos de Gürses e Del Alamo (2016), Alshammari e Simpson (2017a), Hadar *et al.* (2018), Veseli *et al.* (2019), Baldassarre *et al.* (2020) e Bu *et al.* (2020).

Neste contexto, os objetivos da pesquisa foram definidos, como apresentados no Capítulo 1, sendo o objetivo geral **propor um processo de desenvolvimento de software para auxiliar equipes na implementação dos princípios do *Privacy by Design***, e os objetivos específicos: criar um repositório de instâncias de padrões de privacidade; mapear os padrões de privacidade aos princípios fundamentais do PbD;

conceber um processo que considere os princípios fundamentais do PbD; e avaliar o processo proposto.

3.1.3 Projeto e Desenvolvimento

A atividade de Projeto e Desenvolvimento visa a criação do artefato proposto que, segundo Peffers *et al.* (2007), pode ser constructos, modelos, métodos ou instanciações. No contexto desta pesquisa, o artefato solução é um processo de desenvolvimento de software, apoiado pelo papel responsável pela correta execução das etapas do processo e os artefatos de entrada e saída de cada etapa.

O processo proposto, denominado Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP) tem como objetivo integrar a privacidade de dados pessoais dos titulares desde as etapas iniciais de desenvolvimento de software, conforme menciona os princípios fundamentais do PbD (CAVOUKIAN, 2009a). Além disso, o processo conta com dois artefatos: (i) Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design*, e (ii) Repositório de Instâncias de Padrões de Privacidade.

O mapeamento tem como objetivo aproximar os princípios do PbD com as atividades práticas da Engenharia de Software. Realizou-se um mapeamento (ANDRADE *et al.*, 2024) entre os 72 (setenta e dois) padrões de privacidade catalogados pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024) e os 7 (sete) Princípios do PbD (CAVOUKIAN, 2009a). O mapeamento foi realizado pelo autor da presente pesquisa e mais dois especialistas, que realizaram individualmente o mapeamento em ciclos. Ao final de cada ciclo, foram realizadas reuniões nas quais foram discutidos pontos conflitantes para chegar a um consenso sobre o resultado final do mapeamento.

O repositório visa exemplificar a utilização de cada padrão de privacidade para facilitar sua compreensão pelos desenvolvedores de software. Para o desenvolvimento deste artefato utilizou-se cenários reais enfrentados por desenvolvedores de software que podem ser resolvidos por intermédio de um ou mais padrões de privacidade.

Ao final do processo, o artefato gerado é uma História de Usuário considerando os critérios de aceite de privacidade de dados pessoais, como dados pessoais coletados, dados pessoais sensíveis coletados, tempo de retenção dos dados

pessoais coletados, restrições, leis e regulamentos seguidos e recomendações de padrões de privacidade. O processo está descrito em detalhes no Capítulo 6.

3.1.4 Demonstração

A atividade de Demonstração consiste na coleta de dados por meio de entrevistas semiestruturadas com especialistas com experiência em privacidade e proteção de dados pessoais e processos de desenvolvimento de software.

Para a realização desta atividade, um roteiro semiestruturado foi elaborado com base no *Technology Acceptance Model (TAM 3)* (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008) a fim de verificar a percepção de facilidade de uso, utilidade e intenção de uso futuro. A atividade de Demonstração é subdividida em três etapas, sendo definição do escopo, planejamento e execução.

Definição do Escopo: nesta etapa foram definidos o escopo das demonstrações que seriam realizadas.

- **Analisar** o processo, seus artefatos e papel;
- **Com o propósito de** avaliá-los e melhorá-los;
- **Em relação à** percepção da utilidade, facilidade e intenção de uso futuro com base no *Technology Acceptance Model* (TAM 3) (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008);
- **Do ponto de vista de** especialistas com experiência em privacidade e proteção de dados pessoais e processos de desenvolvimento de software. Como é um processo de análise qualitativa, foi selecionado um grupo de especialistas e, ao longo da etapa de entrevistas, realizou-se uma pré-análise iterativa dos dados. O número exato de entrevistados foi definido durante este processo de coleta de dados, quando informações fornecidas por novos especialistas entrevistados acrescentavam pouco ao material já obtido. Assim, segundo Charmaz (2006), considerou-se que as categorias estavam saturadas;
- **No contexto de** profissionais que atuam na indústria em organizações de diferentes portes e domínios.

Planejamento: nesta etapa foram definidos os perfis dos especialistas e a instrumentação da avaliação:

- **Especialistas:** profissionais que possuem conhecimento e experiência em privacidade e proteção de dados pessoais, processos de desenvolvimento e implementação de requisitos envolvendo leis e/ou regulamentos, como por exemplo, Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018a).
- **Instrumentação:** um convite via e-mail foi enviado a cada especialista. Neste e-mail constavam em anexo a Carta de Apresentação (Apêndice A.1), Termo de Compromisso de Utilização de Dados (TCUD) (Apêndice A.2), Termo de Consentimento Livre e Esclarecido (TCLE) (Apêndice A.3), e Questionário de Caracterização de Perfil (Apêndice A.4).

Execução: nesta etapa ocorreu a execução da coleta dos dados referentes a condução da avaliação empírica. Com aceite e preenchimento dos formulários por parte do especialista, o pesquisador entrou em contato a fim de agendar uma reunião para realizar a entrevista semiestruturada intermediada pela plataforma Google Meet[22].

As entrevistas foram gravadas, porém, todas as providências foram tomadas durante a coleta de dados para garantir a privacidade e anonimato do entrevistado. Ao fim da coleta de dados, o nome do entrevistado foi removido e não foi utilizado em nenhum momento durante a análise ou apresentação dos resultados.

O roteiro e as entrevistas semiestruturadas são apresentados de maneira detalhada no Capítulo 7.

3.1.5 Avaliação

A avaliação dos resultados dos estudos empíricos envolveu a transcrição completa das entrevistas conduzidas com especialistas. Essas transcrições foram registradas em documentos no Microsoft Word[23] (.doc) e analisadas individualmente.

[22] Site Google Meet: https://meet.google.com/
[23] Site Microsoft Word: https://www.microsoft.com/pt-br/microsoft-365

Após finalizar a etapa de transcrição, os documentos foram importados na ferramenta ATLAS.ti[24], utilizada para apoiar na organização do processo de análise e codificação das respostas. Entretanto, ressalta-se que a ferramenta ATLAS.ti não interpreta os dados de maneira automatizada, sendo de responsabilidade do pesquisador realizar a análise e interpretação dos dados, os quais foram realizados por meio de método de codificação.

Para realizar a análise e interpretação das respostas de cada entrevistado para as questões abertas, optou-se pela Codificação Provisória (SALDAÑA, 2013), pois ela permite a investigação exploratória por meio de uma lista inicial de códigos pré-estabelecidos sob a percepção TAM 3. Deste modo, sete códigos foram definidos: facilidade de uso, utilidade, intenção de uso futuro, aspectos positivos, limitações, recomendações de uso e sugestões de melhorias, sendo os três primeiros referentes ao TAM 3.

- **Facilidade de uso:** avalia o quão fácil e intuitivo é o uso do processo proposto sob a percepção dos especialistas com base no TAM 3;
- **Utilidade:** avalia se o processo proposto é útil para ser adotado ou adaptado em projetos no meio industrial;
- **Intenção de uso futuro:** verifica se o especialista possui intenção de utilizar o processo proposto em futuros projetos industriais;
- **Aspectos Positivos:** discorrem sobre as principais qualidades encontradas no processo, papel ou artefatos propostos;
- **Limitações:** descrevem os obstáculos enfrentados pelos especialistas em relação ao processo, papel ou artefatos propostos;
- **Recomendações de Uso:** avalia as chances de o especialista recomendar o processo à sua equipe ou a outros engenheiros de software;
- **Sugestões de melhorias:** possibilita ao especialista identificar sugestões e aprimoramento no processo, papel ou artefatos propostos, os quais foram analisados e, quando considerados viáveis, implementadas ao processo a fim de aprimorá-lo.

[24] Site ATLAS.ti: https://atlasti.com/

Os códigos definidos foram associados à trechos de texto ou citações identificados nas respostas dos entrevistados, o que garante a rastreabilidade de evidências para a avaliação qualitativa (SALDAÑA, 2013). Uma vez finalizada esta etapa, os códigos foram refinados e representados graficamente por meio do recurso de redes da ferramenta ATLAS.ti.

A análise dos dados, bem como a codificação e redes geradas a partir das transcrições das entrevistas semiestruturadas, são detalhadas no Capítulo 7.

3.1.6 Comunicação

Na etapa de Comunicação serão apresentados à comunidade científica os resultados da presente pesquisa. Além do documento referente a tese de doutorado, artigos científicos foram redigidos e publicados considerando não só com os resultados obtidos, mas também os problemas iniciais encontrados na literatura.

Com o intuito de investigar como os princípios fundamentais do *Privacy by Design* estão sendo aplicados na área da Engenharia de Software, foi publicada uma Revisão Sistemática da Literatura no *Symposium on Software Quality* (ANDRADE *et al.*, 2022).

Para compreender como a privacidade dos dados pessoais tem sido integrada no processo de desenvolvimento de software das organizações e quais são as dificuldades associadas a esta integração, um estudo de caso foi realizado com 5 organizações de diferentes domínios e portes, e publicado na *International Conference on Computer and Information Technology* (ANDRADE *et al.*, 2023).

Com o propósito de integrar os princípios do *Privacy by Design* às práticas da Engenharia de Software, realizou-se um mapeamento entre os 7 (sete) princípios do PbD com os 72 (setenta e dois) padrões de privacidade catalogados pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024). Este estudo foi publicado na *Ibero-American Conference on Software Engineering* (ANDRADE *et al.*, 2024)

3.2 Considerações sobre o Capítulo

Neste capítulo foi delineada a estrutura desta pesquisa em termos dos métodos adotados, os quais foram fundamentados por atividades da *Design Science Research Methodology (DSRM)*.

CAPÍTULO 4 - PRINCÍPIOS DO PRIVACY BY DESIGN E A ENGENHARIA DE SOFTWARE

De acordo com Cavoukian (2012a), o próximo estágio na evolução do *Privacy by Design* (PbD) é “traduzir os 7 Princípios Fundamentais do PbD em requisitos concretos e prescritivos, especificações, padrões, melhores práticas e critérios de desempenho operacional”. A partir desse cenário, que impacta fortemente todo o ciclo de desenvolvimento de software, surgiu o interesse em realizar uma Revisão Sistemática da Literatura (RSL) para mapear os avanços na área de Engenharia de Software no que diz respeito à exigência do uso dos princípios fundamentais do PbD.

Este capítulo apresenta sucintamente a RSL, que foi conduzida seguindo as diretrizes propostas por Kitchenham e Charters (2007) e Petersen *et al.* (2015). A RSL completa está disponível em Andrade *et al.* (2022).

4.1 Definição dos Objetivos e das Questões de Pesquisa

A RSL considerou artigos disponíveis até o mês de maio de 2022 e tinha como objetivo **mapear as informações obtidas em estudos primários sobre os avanços da Engenharia de Software em relação aos princípios fundamentais do *Privacy by Design***. Para isto, três Questões de Pesquisa (QP) foram definidas:

- QP1: Em quais áreas da Engenharia de Software há contribuições de estudos?

  Esta questão de pesquisa procurou identificar em quais áreas de conhecimento da Engenharia de Software, de acordo com o *Software Engineering Body of Knowledge (SWEBOK)* (BOURQUE; FAIRLEY, 2014), as pesquisas estão sendo conduzidas.

- QP2: Quais são os domínios utilizados nos estudos primários selecionados para realizar teste ou validação do estudo?

  O respeito com a privacidade dos dados dos titulares deve ocorrer independente do domínio da aplicação. Porém, há alguns domínios críticos, por exemplo, sistemas de saúde, pois envolvem dados

sensíveis. Neste contexto, esta questão de pesquisa tinha como objetivo identificar quais domínios estão sendo abordados nos estudos primários.

- QP3: Quais são os artefatos gerados para facilitar a aplicação dos princípios de privacidade no contexto da Engenharia de Software?

  Conforme relatado por Baldassarre *et al.* (2019, 2020), Perera *et al.* (2020), entre outros, existem dificuldades em integrar os princípios de privacidade ao desenvolvimento de softwares, pois há falta de metodologias capazes de realizar tal integração. Portanto, esta questão de pesquisa visava identificar quais artefatos foram propostos pelos estudos primários selecionados.

4.2 Estratégia de Pesquisa

A Figura 4 ilustra todos os passos para a realização da RSL.

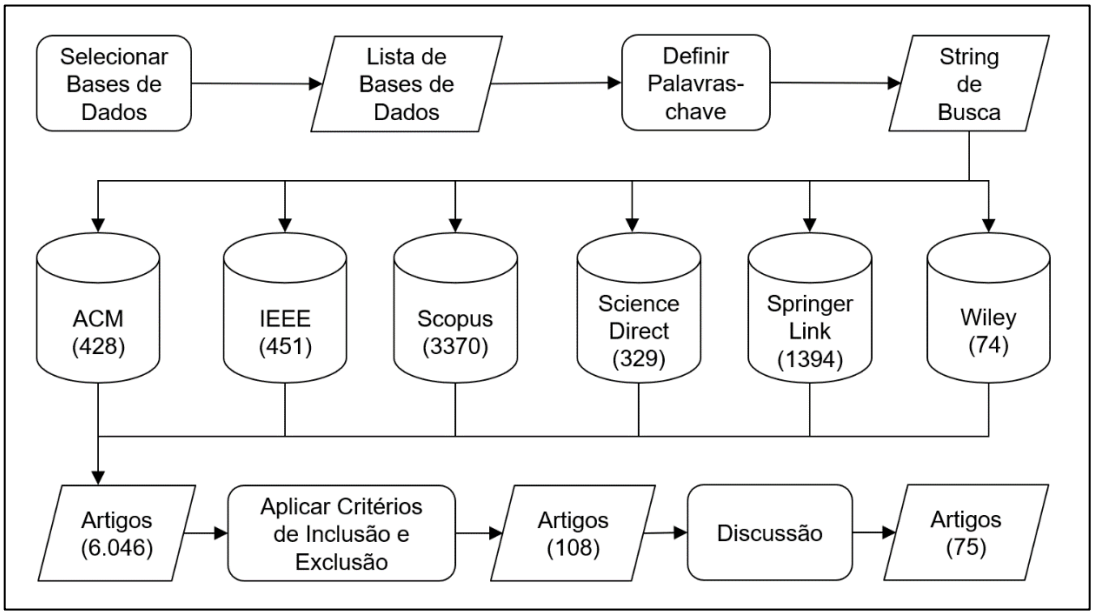

Figura 4. Estratégia de Pesquisa.

Ao todo, seis bases científicas foram consideradas para pesquisar os estudos primários: ACM Digital Library[25]; IEEE Xplore Digital Library[26]; SCOPUS[27], Science Direct[28]; Springer Link[29]; e Wiley Online Library[30].

[25] Site ACM Digital Library: https://dl.acm.org/
[26] Site IEEE Xplore Digital Library: https://ieeexplore.ieee.org/Xplore/home.jsp
[27] Site SCOPUS: https://www.scopus.com/home.uri
[28] Site Science Direct: https://www.sciencedirect.com/
[29] Site Springer Link: https://link.springer.com/
[30] Site Wiley Online Library: https://onlinelibrary.wiley.com/

Após a escolha das bases científicas, as palavras-chave foram especificadas para comporem as *strings* de busca, que não considerou restrições de ano de publicação dos estudos. Contudo, não há como definir uma *string* genérica capaz de ser utilizada em todas as bases, para isto, a *string* de busca precisou ser adaptada para cada uma das bases citadas. O Quadro 1 apresenta as *strings* de busca utilizadas em cada uma das bases e o número total de trabalhos recuperados, respectivamente.

Quadro 1. Número Total de Trabalhos Recuperados.

Base de dados	***String* de pesquisa**	**Número de trabalhos recuperados**
ACM Digital Library	AllField:("Privacy by Design") AND (AllField:("software engineering") OR AllField:("information systems") OR AllField:("software development"))	428
IEEE Xplore Digital Library	("Full Text & Metadata":"Privacy by Design" AND ("Full Text & Metadata":"software engineering" OR "Full Text & Metadata":"software development" OR "Full Text & Metadata":"information systems"))	451
SCOPUS	ALL("Privacy by Design" AND ("software engineering" OR "software development" OR "information systems")) AND (LIMIT-TO(SUBJAREA, "COMP"))	3.370
Science Direct	"Privacy by Design" AND ("software engineering" OR "information systems" OR "software development")	329
Springer Link	"Privacy by Design" AND ("software engineering" OR "information systems" OR "software development")	1.394
Wiley Online Library	"Privacy by Design" AND ("software engineering" OR "information systems" OR "software development")	74
TOTAL		**6.046**

A busca nas bases de dados resultou em um total de 6.046 artigos. Após a eliminação dos títulos duplicados, obteve-se um total de 5.479 artigos. Durante o processo de revisão por pares, foram selecionados 108 artigos aplicando-se os critérios de inclusão e exclusão.

Após a fase de discussão para consenso entre os pesquisadores, foram excluídos 33 artigos, pois não respondiam às questões de pesquisa, resultando em 75 estudos primários selecionados. Ressalta-se que a pesquisa ocorreu em bases de dados científicas que retornaram apenas artigos publicados em periódicos ou conferências. Neste caso, não foram considerados resumos e teses. O conjunto final de metadados dos estudos primários selecionados são apresentados em sua totalidade no Quadro 10 do Apêndice B.

As etapas do processo de revisão foram realizadas em pares e foi calculado o Coeficiente Kappa[31] de concordância entre os pesquisadores. Quando houve divergência entre eles, foi realizada uma reunião para discussão e consenso. A estatística Kappa retornada foi de 0,748 (74,8%), o que significa uma concordância substancial entre os revisores (LANDIS; KOCH, 1977).

Em seguida, os pesquisadores que conduziram o processo de seleção dos estudos primários, realizaram a classificação dos artigos segundo:

i. O tipo de pesquisa, com base nas categorias propostas por Wieringa (2006): pesquisas de validação, pesquisas de avaliação, uma solução, artigos filosóficos, artigos de opinião e artigos de experiência pessoal;
ii. As áreas de conhecimento do *Software Engineering Body of Knowledge (SWEBoK)* (BOURQUE; FAIRLEY, 2014); e
iii. As categorias utilizadas por Morales *et al.* (2019): ferramentas, teoria, métodos, modelos, padrões e prática profissional.

Por fim, a categorização da codificação resultante permitiu realizar a análise descritiva. Os resultados encontram-se na Seção 4.3. O Quadro 11 do Apêndice C apresenta a síntese dos dados extraídos dos estudos primários selecionados.

4.3 Visão Geral dos Estudos Primários Selecionados

A Figura 5 ilustra a distribuição das publicações por ano e tipo. Os 75 estudos primários selecionados foram de 2011 a maio de 2022. Destes, 54 (72%) foram publicados em conferências, 18 (24%) em periódicos e 3 (4%) como capítulos de livros. É possível observar um aumento no número de publicações a partir de 2014, sendo 2018 o ano com maior número de estudos publicados, 11 no total. Este aumento de publicações pode estar relacionado ao interesse e necessidade da comunidade de Engenharia de Software em avançar nas pesquisas devido à liberação do *General Data Protection Regulation (GDPR)*.

[31] O Coeficiente Kappa é uma medida estatística de concordância entre avaliadores para itens qualitativos.

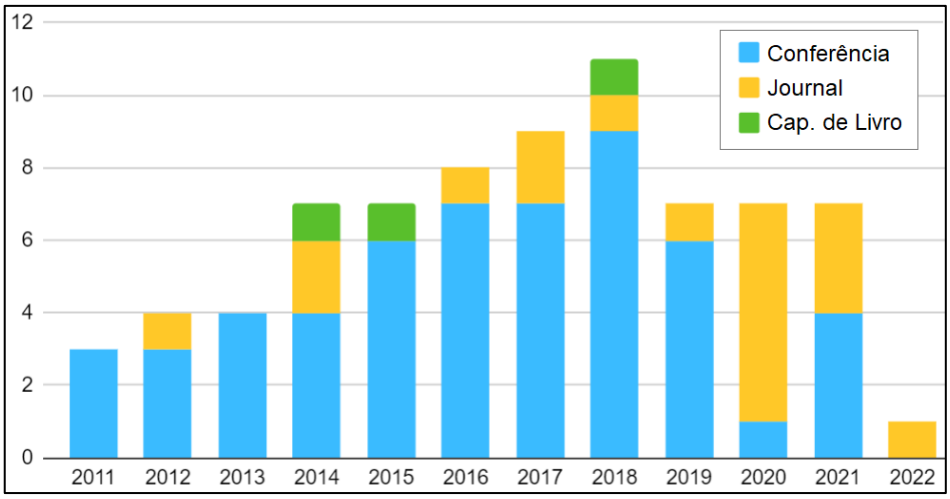

Figura 5. Distribuição dos Estudos Primários por Ano de Publicação.

Os artigos foram classificados de acordo com as categorias propostas por Wieringa (2006). A Figura 6 (Página 47) ilustra a distribuição dos tipos de pesquisa em cada área de conhecimento da Engenharia de Software, definida no SWEBoK (BOURQUE; FAIRLEY, 2014). Segue uma breve análise descritiva dos tipos de pesquisa que estão sendo realizados:

- **Proposta de Solução:** 35 artigos (46,67%). Este número elevado destaca a falta de métodos sistemáticos que traduzam os princípios do PbD em diretrizes para o processo de desenvolvimento de software, conforme relatado por (BALDASSARRE *et al.*, 2020; BU *et al.*, 2020; VESELI *et al.*, 2019);
- **Artigos Filosóficos:** 24 artigos (32%) discutem como os princípios do GDPR, ou regulamentos similares, podem ser derivados em requisitos para o desenvolvimento de softwares (GUERRIERO *et al.*, 2017);
- **Pesquisa de Avaliação:** 7 artigos (9,33%) investigam problemas ou implementações do PbD na prática. As propriedades são verificadas empiricamente por meio de estudos de caso, experimentos e *surveys*;
- **Pesquisa de Validação**: 5 artigos (6,67%) apresentam propostas de soluções que ainda não foram implementadas na prática. Esta categoria inclui estudos que propõem protótipos, *frameworks* e análises formais;
- **Artigos de Opinião:** 4 artigos (5,33%) se posicionam sobre abordagens específicas ou estudos de caso e desafios encontrados.

Durante a análise, observou-se que 68 estudos citam outros princípios de privacidade contidos em normas e/ou regulamentos além dos princípios do PbD. Entre os mais citados: *General Data Protection Regulation (GDPR)*, com 48 citações; *Data Protection Directive 95/46/EC*, com 24 citações, *Organization for Economic Cooperation and Development (OECD) Guidelines*, com 19 citações; *ISO/IEC 29.100*, com 15 citações; *Health Insurance Portability and Accountability Act (HIPAA)*, com 7 citações; *Global Privacy Standard (GPS)*, com 4 citações; *UK Data Protection Act (UKDPA)*, com 3 citações; *Accepted Privacy Principles (GAPPs)*, com 2 citações; Lei Geral de Proteção de Dados Pessoais (LGPD), com 1 citação; e outras normas/regulamentos que somam 59 citações.

Existem muitas citações ao GDPR de 2014 porque, embora o GDPR tenha sido aprovado em 2016, suas primeiras propostas ocorreram em meados de 2012. O GDPR é o regulamento atual na União Europeia e revogou a *Data Protection Directive 95/46/EC*, a segunda regulação mais citada nos estudos primários selecionados.

4.3.1 Contribuições na Área de Engenharia de Software

Os estudos foram classificados de acordo com as áreas de conhecimento definidas no SWEBoK (BOURQUE; FAIRLEY, 2014). Foram identificados artigos em 4 áreas, sendo: 23 em Requisitos de Software (30,66%), 17 em Projeto de Software (22,67%), 13 em Processo de Engenharia de Software (17,33%) e 5 em Construção de Software (6,67%). Para os 17 estudos (22,67%) que não se enquadravam em nenhuma área específica foi atribuída a categoria Geral, conforme Figura 6.

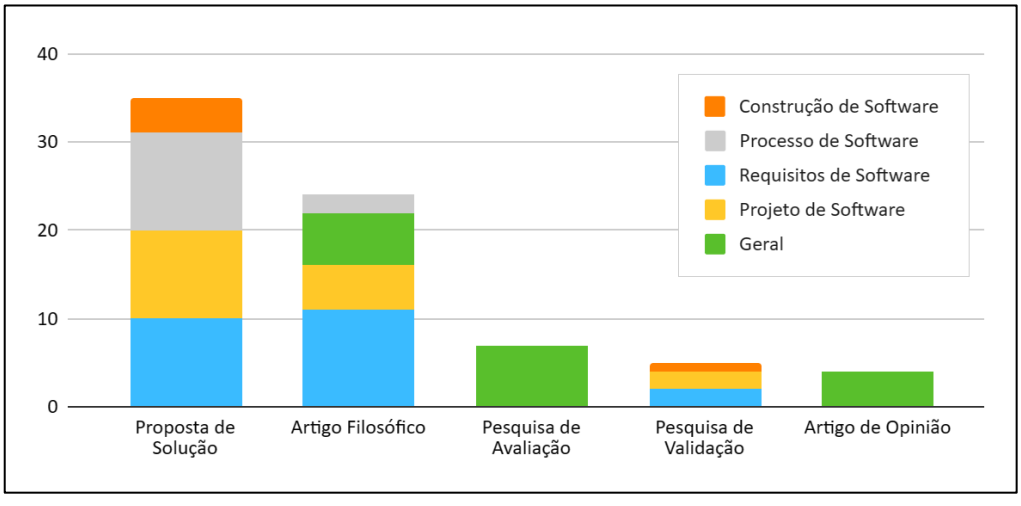

Figura 6. Artigos de acordo com as Áreas de Conhecimento SWEBoK.

Os estudos na área de Requisitos de Software propõem principalmente abordagens para ajudar os engenheiros de software a especificar aplicações sensíveis à privacidade. Exemplos de artigos nesta categoria incluem Tamburri (2020), que descreve *insights* sobre como reduzir despesas com requisitos de privacidade nos estágios iniciais de desenvolvimento de software, e Rygge e Jøsang (2018), que apresenta um jogo para incentivar os desenvolvedores a considerar os requisitos de privacidade ao avaliar, remover ou mitigar vulnerabilidades.

A categoria Projeto de Software inclui estudos que visam criar especificações para um artefato de software. Alguns exemplos de artigos nesta categoria são Colesky *et al.* (2018), que apresenta padrões de privacidade para controle do usuário, e Amankona *et al.* (2021), que propõe um *framework* de privacidade para sistemas e-Health[32] para melhorar a privacidade e a segurança da informação no setor de saúde.

Na categoria Geral estão artigos *survey* e discussão, como o estudo de Bu *et al.* (2021), que examina quais fatores influenciam os engenheiros de software a implantar princípios PbD em projetos de software, e Galvez e Gurses (2018), que explora os desafios e oportunidades introduzidos na modelagem de ameaças à privacidade, combinando metodologias ágeis e arquiteturas orientadas a serviços.

Na categoria Processos de Engenharia de Software alguns estudos propõem abordagens e métodos que visam auxiliar as equipes em todas as etapas do desenvolvimento de software. Alguns exemplos são os estudos de Baldassarre *et al.* (2020), em que os autores apresentam o *Privacy Oriented Software Development (POSD)*, uma abordagem que suporta requisitos de privacidade e segurança no desenvolvimento de software, e Sakul-Ung e Smanchat (2019) que apresenta um *framework* capaz de gerenciar, desenvolver e monitorar mecanismos de proteção à privacidade em projetos de desenvolvimento de software.

A categoria Construção de Software envolve estudos que detalham o software funcional obtido por meio de codificação, verificação e testes. Exemplos de artigos nesta categoria incluem os estudos de Guerriero *et al.* (2017), que apresenta uma ferramenta que permite aos designers especificar modelos de arquitetura para suas próprias aplicações, e Rowan e Dehlinger (2014), que apresenta um *plugin*,

[32] E-Health: descreve serviços de saúde apoiados por processos digitais, comunicação ou tecnologia, como prescrição eletrônica, telemedicina ou registos de saúde eletrônicos (DELLA MEA, 2001).

denominado *Policy AutoGeneration in Eclipse (PAGE)*, para integrar recursos de planejamento de privacidade no Eclipse IDE[33].

4.3.2 Domínio de Aplicação dos Estudos Primários

Em relação aos domínios utilizados nos estudos primários selecionados para realizar teste ou validação do estudo, 52 artigos (69,33%) mencionaram um ou mais domínios utilizados na pesquisa. O Quadro 2 apresenta os estudos primários por domínio da aplicação.

Quadro 2. Domínios de Aplicação dos Estudos Primários Selecionados.

Domínios da Aplicação	Estudos Primários Selecionados
Saúde	Gaudino (2011); Jutla *et al.* (2013); Stevovic *et al.* (2015a); Stevovic *et al.* (2015b); Kolkowska (2015); Siljee (2015); Colesky e Ghanavati (2016); Aljohani *et al.* (2016); Trujillo e Mireles (2018); Romanou (2018); Senarath e Arachchilage (2018); Piras *et al.* (2019); Hatamian (2020); Semantha *et al.* (2021); Amankona *et al.* (2021).
Domínio Genérico	Ahmadian *et al.* (2019); Bargh e Choenni (2019); Degeling *et al.* (2016); Hadar *et al.* (2018); Oetzel e Spiekermann (2012); Pedroza *et al.* (2021); Shishkov e Janssen (2018); Baldassarre *et al.* (2021).

[33] Eclipse IDE: Ambiente de Desenvolvimento Integrado (IDE) Java. Entretanto, utilizado para outras linguagens de programação, como C/C++, JavaScript/TypeScript, PHP, entre outras (ECLIPSE FOUNDATION, 2023).

Serviços Online	Baldassarre *et al.* (2019); Baldassarre *et al.* (2020); Dodero *et al.* (2019); Senarath *et al.* (2017); Vemou e Karyda (2014).
Sistemas de Pedágio	Alshammari e Simpson (2017b); Alshammari Simpson (2018); Kung (2014); Kung *et al.* (2011); Le Métayer (2013).
Internet da Coisas (IoT)	Bugeja e Jacobsson (2020); Foukia *et al.* (2016); Perera *et al.* (2020); Perera *et al.* (2016).
Sistemas de Vigilância	Chandramouli *et al.* (2013); Kung *et al.* (2015); Romanou (2018).
Energia	Morton e Sasse (2012); Piras *et al.* (2019); Vaidya e Mouftah (2018).
Big Data	Guerriero *et al.* (2017); Jutla *et al.* (2013).
Sistemas de Autenticação	Hörbe e Hötzendorfer (2015); Romanou (2018).
Sistemas de Transporte Inteligentes	Kost *et al.* (2011); Righini *et al.* (2022).
E-Commerce	Alharbi *et al.* (2012).
Sistema Bancário	Ali *et al.* (2016).
Sistema Educacional	Hoel *et al.* (2017).

O domínio de saúde apresenta o maior número de citações (15 citações). Um possível motivo é porque possui dados que devem ter tratamento especial, conforme definido no Art. 9 do GDPR. Consequentemente, há uma maior preocupação com a privacidade desses dados.

Em 8 estudos primários, suas contribuições podem ser utilizadas em qualquer domínio. Os domínios de Serviços Online possuem 5 citações (9,62%), apresentando sistemas como redes sociais, web e aplicativos móveis em geral, que apresentam riscos à privacidade por coletarem constantemente informações de seus usuários.

Os sistemas de pedágio foram citados em 5 estudos (9,62%), com foco na coleta de informações de localização dos automóveis e de seus proprietários. As demais citações foram distribuídas nos domínios: Internet das Coisas (IoT) (4 citações), Sistemas de Vigilância, Energia (3 citações cada), *Big Data*, Sistemas de Autenticação, Sistemas de Transporte Inteligentes, com 2 citações cada, *E-Commerce*, Sistema Bancário e Sistema Educacional, 1 citação cada.

4.3.3 Artefatos Gerados para Facilitar a Aplicação dos Princípios de Privacidade na Engenharia de Software

Com o intuito de descobrir quais tópicos estão entre os mais discutidos e quais necessitam de atenção para pesquisas futuras, os estudos foram classificados em seis categorias de acordo com o artefato gerado (MORALES-TRUJILLO *et al.*, 2019):

- **Teórico:** estudos que apresentem *insights* teóricos sobre como os conceitos de privacidade devem ser implementados na Engenharia de Software;
- **Modelo:** consideram fatores, como dimensões sociais, que influenciam a implementação da privacidade nos sistemas;
- **Padrão:** discorrem sobre padrões de projetos de privacidade;
- **Método:** *frameworks* ou métodos que se preocupam com a implementação, de modo sistemático, da privacidade durante a elicitação de requisitos ou contemplando diversas etapas do ciclo de desenvolvimento de software;
- **Ferramenta:** estudos que apresentam protótipos, metamodelos ou linguagens formais na validação de suas ferramentas; e
- **Prática Profissional:** apresentam resultados práticos relacionados à privacidade de dados na perspectiva dos *stakeholders*.

Considerando essa classificação, 24 artigos (32%) foram categorizados como modelo, 15 (20%) como teóricos, 15 artigos (20%) como método, 9 (12%) como padrão, 6 (8%) como ferramenta e 6 (8%) como prática profissional. O Quadro 3 apresenta a distribuição dos artigos por artefatos gerados e o tipo de pesquisa desenvolvida.

Quadro 3. Artefatos Gerados para Facilitar a Aplicação dos Princípios de Privacidade no Contexto da Engenharia de Software.

Artefato Gerado	Tipo de Pesquisa	Estudos Primários Selecionados
Teórico	Artigo Filosófico	Galvez e Gurses (2018); Romanou (2018); Vaidya e Mouftah (2018); Hörbe e Hötzendorfer (2015); Kolkowska (2015); Chen e Williams (2013); Van Rest *et al.* (2014); Notario *et al.* (2014); Hazeyama *et al.* (2016); Lenhard *et al.* (2017).
	Artigo de Opinião	Gaudino (2011); Kung *et al.* (2011); Spiekermann (2012); Schneide (2018).
	Pesquisa de Avaliação	Ayalon e Toch (2021).
Modelo	Proposta de Solução	Morton e Sasse (2012); Vemou e Karyda (2014); Kung *et al.* (2015); Foukia *et al.* (2016); Perera *et al.* (2016); Blix *et al.* (2017); Alshammari e Simpson (2017c); Shishkov e Janssen (2018); Trujillo e Mireles (2018); Alshammari Simpson (2018); Al-Momani *et al.* (2019); Sakul-Ung e Smanchat (2019); Semantha *et al.* (2021); Amankona *et al.* (2021).

	Artigo Filosófico	Chandramouli *et al.* (2013); Martín *et al.* (2014); Degeling *et al.* (2016); Hoel *et al.* (2017); Bargh e Choenni (2019); Tamburri (2020); Hatamian (2020).
	Pesquisa de Validação	Kost *et al.* (2011); Le Métayer (2013).
	Pesquisa de Avaliação	Perera *et al.* (2020).
Padrão	Proposta de Solução	Kung (2014); Siljee (2015); Ali *et al.* (2016); Colesky e Ghanavati (2016).
	Artigo Filosófico	Hoepman (2014); Colesky *et al.* (2016); Aljohani *et al.* (2016); Caiza *et al.* (2017); Colesky *et al.* (2018).
Método	Proposta de Solução	Stevovic *et al.* (2015a); Stevovic *et al.* (2015b); Senarath *et al.* (2017); Rygge e Jøsang (2018); Baldassarre *et al.* (2019); Ahmadian *et al.* (2019); Dodero *et al.* (2019); Baldassarre *et al.* (2020); Bugeja e Jacobsson (2020); Peixoto (2020); Pedroza *et al.* (2021); Baldassarre *et al.* (2021).
	Artigo Filosófico	Notario *et al.* (2015); Alshammari e Simpson (2017a).
	Pesquisa de Validação	Oetzel e Spiekermann (2012).

Ferramenta	Proposta de Solução	Jutla *et al.* (2013); Rowan e Dehlinger (2014); Alshammari e Simpson (2017b); Piras *et al.* (2019); Righini *et al.* (2022).
	Pesquisa de Validação	Guerriero *et al.* (2017).
Prática Profissional	Pesquisa de Avaliação	Alharbi *et al.* (2012); Hadar *et al.* (2018); Senarath e Arachchilage (2018); Bu *et al.* (2020); Bu *et al.* (2021); Tahaei *et al.* (2021).

A literatura mostra que a maioria dos estudos (54 estudos, 72%) visa discutir teoricamente os conceitos de privacidade, mapeando os elementos que influenciam a implementação de sistemas de privacidade, e como fazê-lo. Portanto, faltam estudos empíricos envolvendo os princípios do PbD e, ainda, implementação prática com *stakeholders*.

Embora os 75 estudos selecionados estejam diretamente relacionados ao PbD e à Engenharia de Software, 48 (64%) não citam os princípios do PbD. Consequentemente, não há informações sobre como esses princípios podem ser abordados na Engenharia de Software. Em contraste, os outros 27 artigos possuem alguma referência direta a pelo menos um princípio do PbD. No entanto, constatou-se que muitos destes princípios não foram totalmente integrados nos métodos/processos propostos, como o princípio da Funcionalidade Total, que ainda compete com outras funcionalidades do sistema num resultado de soma zero.

4.4 Trabalhos Relacionados

Dentre os diversos estudos encontrados na literatura envolvendo privacidade e proteção de dados pessoais, 16 (dezesseis) são considerados relacionados ao tema desta tese e são apresentados no Quadro 4.

Quadro 4. Trabalhos Relacionados entre PbD e Engenharia de Software Comparados com o Processo Proposto.

Autor(es)	Princípios do PbD	Mapeamento dos Princípios do PbD em atividades da Engenharia de Software	Elementos utilizados	Processo de Desenvolvimento				Domínio da Solução Proposta		Ferramenta Desenvolvida
				Tradicional	Iterativo	Ágil	Genérico	Específico	Geral	
Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP)	✓	✓	Privacy Patterns	-	-	-	✓	-	✓	Repositório PDSOP
Viitaniemi (2017)	✓	-	-	-	-	✓	-	-	✓	-
Peixoto (2021)	-	-	-	-	-	✓	-	-	✓	Privacy Criteria Method Tool
Rygge; Jøsang (2018) *	-	-	-	-	-	✓	-	-	✓	-
Baldassarre *et al.* (2020)	✓	✓	Privacy Design Strategies Privacy Patterns	✓	-	-	-	-	✓	Privacy Knowledge Base (PKB)
Perera *et al.* (2020)	✓	✓	Privacy Design Strategies	-	-	-	-	✓	-	-
Stevovic *et al.* (2015b)	-	-	-	-	✓	-	-	✓	-	CHINO platform
Notario *et al.* (2014) *	-	-	Privacy Impact Analysis Privacy-Enhancing Technologies	-	-	-	-	-	✓	PRIPARE
Alshammari; Simpson (2018)	-	-	Privacy Patterns Privacy-Enhancing Technologies	-	-	-	-	✓	-	-

Autor(es)	Princípios do PbD	Mapeamento dos Princípios do PbD em atividades da Engenharia de Software	Elementos utilizados	Processo de Desenvolvimento				Domínio da Solução Proposta		Ferramenta Desenvolvida
				Tradicional	Iterativo	Ágil	Genérico	Específico	Geral	
Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP)	✓	✓	Privacy Patterns	-	-	-	✓	-	✓	Repositório PDSOP
Senarath *et al.* (2017)	-	-	Privacy-Enhancing Technologies	-	✓	-	-	✓	-	-
Al-Momani *et al.* (2019) *	-	-	Privacy Impact Assessment Privacy-Enhanced Architecture	✓	-	-	-	-	✓	-
Sakul-Ung; Smanchat (2019) *	-	-	-	✓	-	-	-	-	✓	-
Ahmadian *et al.* (2019)	-	-	Privacy Design Strategies Privacy Patterns Privacy-Enhancing Technologies	-	-	-	-	-	✓	-
Hoepman (2014)	-	-	Privacy Patterns	-	✓	-	-	-	✓	-
Colesky; Hoepman; Hillen (2016) *	-	-	Privacy Design Strategies Privacy Patterns	-	-	-	-	-	✓	-
Oetzel; Spiekermann (2012)	-	-	Privacy Impact Assessment	-	-	-	-	-	✓	Ferramenta Web
Vemou; Karyda (2014)	✓	-	Privacy Design Strategies	-	-	-	-	✓	-	-

* Trabalhos que não especificam o domínio da solução proposto e foram atribuídos como de domínios gerais.

Viitaniemi (2017), propõe um modelo que insere os princípios do PbD no *framework* Scrum. O estudo citado difere do Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP), pois não fornece um processo para apoiar as atividades de engenharia de requisitos de privacidade, tampouco esclarece como implementar os princípios do PbD em ações práticas no modelo ágil de desenvolvimento. As demais etapas citadas no trabalho de Viitaniemi (2017) são abordadas de maneira superficial e a avaliação do modelo ocorre de maneira não empírica.

Peixoto (2021) propõe um processo, denominado *Privacy Criteria Method* (PCM), que visa orientar os desenvolvedores de software na atividade de especificação de requisitos de privacidade no contexto ágil de desenvolvimento. O processo proposto derivou de um modelo conceitual de privacidade e de um *framework* que abrangem recomendações para garantir a privacidade na engenharia de requisitos. O estudo de Peixoto (2021) se diferencia do PDSOP em alguns fatores. Enquanto o PDSOP utiliza os princípios do PbD e os Padrões de Privacidade como artefatos auxiliares para a escrita de histórias de usuário, o PCM possui um modelo conceitual de autoria da própria autora. Além disso, o PCM é focado na engenharia de privacidade para o contexto ágil de desenvolvimento de software, enquanto o PDSOP pode ser integrado tanto no contexto ágil quanto tradicional de desenvolvimento.

Baldassarre *et al.* (2020) propõe uma abordagem, denominada *Privacy Oriented Software Development (POSD)*, capaz de suportar requisitos de privacidade e segurança e é inspirada no ciclo de vida de desenvolvimento de software apresentado pelo *National Institute of Standards and Technology* (KISSEL *et al.*, 2008). O PDSOP se difere do trabalho de Baldassarre *et al.* (2020) em dois pontos: (i) Baldassarre *et al.* (2020) propõem uma abordagem voltada ao processo de desenvolvimento tradicional de software, envolvendo explicitamente as fases de análise, design, codificação, verificação e validação. Fases estas, inexistentes nos processos ágeis de desenvolvimento de software; e (ii) Baldassarre *et al.* (2020) realizaram o mapeamento de 21 padrões de privacidade em relação às Estratégias de Hoepman (HOEPMAN, 2014) e, posteriormente, as estratégias foram associadas aos princípios do PbD devido às vulnerabilidades encontradas, porém, não deixa explícito quais são as vulnerabilidades e como esta relação foi realizada. No PDSOP, o mapeamento ocorre por meio da relação direta dos princípios do PbD com os

padrões de privacidade. Além disso, foram considerados os 72 padrões de privacidade catalogados pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024).

Perera *et al.* (2020) apresenta diretrizes a partir das estratégias de Hoepman (2014) e as utiliza para aplicar/avaliar recursos de privacidade durante o desenvolvimento de aplicativos IoT. Porém, o próprio autor reconhece que as diretrizes ainda estão em um nível alto de abstração, sendo necessário utilizar um conjunto de táticas, padrões de privacidade e técnicas de interação humano-computador na tentativa de melhoria de seu modelo. O *framework* proposto por Perera *et al.* (2020) fornece um conjunto de diretrizes, porém, não menciona como estão relacionadas com os princípios do PbD; possui foco no domínio de aplicativos IoT; e não especifica o modelo de processo de software utilizado na implementação de aplicativos IoT. O PDSOP utiliza os padrões de privacidade como uma maneira de tornar os princípios do PbD aplicáveis à Engenharia de Software, além disso, a integração do PDSOP pode ser realizada tanto em processos tradicionais quanto ágeis de desenvolvimento de software, e não há limitação do domínio de aplicação.

No estudo de Rygge e Josang (2018) é proposto um jogo, denominado *Threat Poker*. Este jogo de cartas ocorre durante reuniões e visa estimular os desenvolvedores a considerar ameaças de segurança e privacidade e a avaliar maneiras de remover ou mitigar vulnerabilidades relacionadas a essas ameaças. O PDSOP difere do estudo de Rygge e Josang (2018) em três pontos: (i) o método *Threat Poker*, apesar de citar a privacidade de dados, tem foco voltado à segurança do software; (ii) não aborda os princípios do PbD; e (iii) não fornece um método para resolver na prática as ameaças identificadas, sejam de segurança ou privacidade de dados.

Stevovic *et al.* (2015b) propõem um método que inicia com duas atividades paralelas, sendo a identificação dos requisitos de negócio e a identificação dos requisitos de *compliance* das legislações. Com ambas as identificações, são definidos os cenários de gerenciamento de dados com reconhecimento de *compliance*. O analista de negócio combina os requisitos obtidos nas etapas anteriores para elaborar uma representação de alto nível que é traduzida em processos e regras de negócio executáveis. Apesar dos autores mencionarem que esse método pode ser executado iterativamente, não descrevem em detalhes como interagiria com um processo ágil de desenvolvimento. Outra diferença para o PDSOP é que Stevovic *et al.* (2015b) não

descrevem como os princípios do PbD são implementados como atividades práticas em um modelo de processo de software.

Notario *et al.* (2015) relata que engenheiros de software encontram dificuldades em traduzir requisitos abstratos de privacidade e, aliado ao fato de possuir poucas práticas ou abordagens de privacidade, os autores desenvolveram o método PRIPARE, que visa combinar duas abordagens, a orientação a objetivos e a análise de risco. Enquanto a primeira reduz a incerteza de privacidade em um estágio inicial do processo de desenvolvimento, a segunda tem objetivo de identificar o tratamento adequado aos riscos restantes. Esse método sofre algumas críticas, principalmente na abordagem orientada a objetivos, pois a análise é acompanhada de um catálogo de requisitos que precisa ser evoluído e harmonizado com profissionais de privacidade. Apesar da proximidade da metodologia PRIPARE com o PDSOP, destacam-se algumas diferenças: a abordagem PRIPARE, apesar do foco em PbD, não menciona como os princípios são implementados na prática; apesar de citar que a abordagem pode ser utilizada para qualquer domínio de software, não menciona qual modelo de processo a abordagem PRIPARE está baseada, tampouco como inserir os requisitos não funcionais, como privacidade, nas atividades de desenvolvimento de software.

Alshammari e Simpson (2018) propõem uma abordagem que fornece um conjunto de critérios de seleção de táticas arquitetônicas para que sejam descritas por meio de padrões de projeto e implementadas por *Privacy-Enhancing Technologies* (PETs). Contudo, a abordagem de Alshammari e Simpson (2018) se difere do PDSOP, pois os autores não especificam à quais princípios do PbD as táticas arquitetônicas estão relacionadas e não mencionam como a seleção das táticas arquitetônicas propostas se relacionam com um processo de desenvolvimento de software.

Senarath *et al.* (2017) critica abordagens que ignoram as perspectivas dos usuários e características comportamentais ao incorporar a privacidade aos sistemas. Para solucionar este problema, fornece uma abordagem sistemática centrada ao usuário e aplicada ao *Unified Process* (UP) para possibilitar que desenvolvedores de software projetem os requisitos de privacidade à medida que abordam o ciclo de vida de desenvolvimento. Enquanto a abordagem de Senarath *et al.* (2017) utiliza modelo tradicional de desenvolvimento de software, o PDSOP é adaptável tanto ao modelo tradicional quanto ao ágil e, além disso, Senarath *et al.* (2017) não cita os princípios

do PbD e como são mapeados e implementados na prática, enquanto o PDSOP aborda explicitamente os princípios, além de mapeá-los em padrões de privacidade.

Al-Momani *et al.* (2019) apresentam o Modelo W com reconhecimento de privacidade. O PDSOP visa integrar os princípios do PbD no processo de desenvolvimento de software, a fim de introduzir sistemas com privacidade aprimorada por meio da implementação de padrões de privacidade e princípios do PbD. O estudo de Al-Momani *et al.* (2019) considera o modelo tradicional, enquanto o PDSOP não se limita ao modelo tradicional. Outro fator relevante a ser considerado é que Al-Momani *et al.* (2019) considera a avaliação do impacto da privacidade para contemplar os princípios do PbD, porém não menciona como os princípios são ou não contemplados no modelo proposto.

Sakul-Ung e Smanchat (2019) propõem um *framework* integrado ao ciclo de desenvolvimento tradicional de software para gerenciamento de privacidade baseado na tríade pessoas-processo-tecnologia. O PDSOP se difere neste ponto, pois considera processos tradicionais e ágeis de desenvolvimento de software. Além disso, Sakul-Ung e Smanchat (2019) não citam como os princípios do PbD são contemplados no *framework* proposto, tampouco quais são os elementos utilizados na implementação dos princípios.

Ahmadian *et al.* (2019) fornece uma metodologia sistemática baseada em modelos da *Unified Modeling Language* (UML) para apoiar a melhoria da privacidade dos sistemas de TI, abordando riscos, interrelações e custos. Porém, para estimá-los, a abordagem baseia-se em suposições que os esforços podem ser estimados de maneira confiável em termos de métricas de contagem de elementos. A avaliação do modelo conta apenas com três estudos de caso com foco em diagramas de atividades. Apesar do estudo de Ahmadian *et al.* (2019) relacionar padrões de privacidade, tecnologias de aprimoramento da privacidade e estratégias de Hoepman, não cita como os princípios do PbD são contemplados na metodologia, tampouco menciona qual processo de desenvolvimento de software está relacionado com a metodologia proposta.

Hoepman (2014) reconhece a necessidade de desenvolver princípios orientadores para dar suporte aos princípios do *Privacy by Design*. Para preencher esta lacuna, o autor define a estratégia de design de privacidade que descreve abordagens fundamentais para a proteção da privacidade. Colesky *et al.* (2016) reconhece a importância e contribuição das estratégias para aproximar o domínio

jurídico da Engenharia de Software, porém menciona que suas definições originais são amplas e vagas, as quais precisam ser refinadas para serem usadas na prática. Apesar das estratégias de Hoepman (2014) serem um dos principais trabalhos no contexto de privacidade de dados, há diferença entre este estudo e o PDSOP. Hoepman (2014) não deixa explícito como suas 8 (oito) estratégias estão relacionadas com os princípios do PbD. Além disso, propõe a utilização das estratégias envolvendo um modelo iterativo de desenvolvimento. O PDSOP mapeia os princípios do PbD nos padrões de privacidades e pode ser utilizado no contexto genérico de desenvolvimento, não fazendo distinção entre processos iterativos ou ágeis.

Colesky *et al.* (2016) procura redefinir de modo concreto as estratégias de Hoepman por meio de “táticas de design”. As táticas de design formam uma camada adicional de abstração que permitem ao engenheiro de software uma melhor compreensão e classificação da estratégia. Porém, este trabalho é criticado por Alshammari e Simpson (2018), que mencionam que as táticas saltam diretamente de princípios abstratos de privacidade para arquiteturas de software o que, segundo Alshammari e Simpson (2018), é uma inconsistência pelo fato dos princípios de privacidade abstratos serem diferentes de funcionalidades de um sistema concreto. Gürses *et al.* (2015) criticam que as táticas deixam de relatar como podem ser aplicadas na construção de sistemas de preservação da privacidade. Semelhante ao estudo de Hoepman (2014), Colesky *et al.* (2016) não menciona como os princípios do PbD são abordados e mapeados em atividades práticas da Engenharia de Software, também não mencionam quais modelos de processos e como as táticas propostas podem ser utilizadas.

O trabalho de Oetzel e Spiekermann (2012) possui foco nos requisitos de privacidade. Os autores mencionam que as abordagens existentes relacionadas à avaliação do impacto à privacidade possuem problemas de imprecisão e lentidão, e propõem um método que considera sistematicamente as questões de privacidade na etapa de elicitação de requisitos de software. Neste estudo, Oetzel e Spiekermann (2012) não descrevem como os princípios do PbD são contemplados no processo de avaliação do impacto de privacidade, tampouco como e em quais modelos de processos podem ser utilizados.

Por fim, Vemou (2014) reconhece a importância do desenvolvimento de tecnologias que aumentam a privacidade e se baseiam na pesquisa de Hoepman (2014) para criar uma lista de requisitos de privacidade com o intuito de orientar o

projeto de plataformas de serviços de redes sociais. Apesar de citarem os princípios do PbD, não deixam explícito como são mapeados para atividades práticas da Engenharia de Software, além de não mencionar como a lista de requisitos pode ser aplicada e em quais processos de desenvolvimento.

4.4.1 Iniciativas Globais para Aplicar PbD em Processos de Desenvolvimento de Software

Há diversas propostas empíricas com o intuito de aplicar os princípios do PbD em processos de desenvolvimento de software, porém, ainda necessitam ser melhor detalhadas e estudadas cientificamente a fim de validar os modelos propostos.

Bozdag (2020) descreve uma solução com foco no problema do App Uber. Nesta solução, o autor menciona categorias de classificações dos níveis de privacidade das informações utilizadas pelo aplicativo, porém não oferece detalhes do processo de desenvolvimento.

Degeling e Loser (2013) apresentam um relato de experiência no desenvolvimento de aplicativos. A abordagem proposta visa apoiar os desenvolvedores por meio de questionamentos de risco de privacidade e fornece uma lista de dicas e práticas recomendadas para possíveis problemas de segurança. Entretanto, a abordagem não ilustra o processo de desenvolvimento e como serão abordados os princípios do PbD.

No trabalho de Driel (2016) é apresentado o *framework* "*Secure Scrum: Development of Secure Software with Scrum*". O autor estabelece uma camada de componentes no *framework* Scrum para garantir a segurança e privacidade que são relacionadas com a história do usuário. Apesar do foco do *framework* estar relacionado à segurança e privacidade, não é mencionado pelo autor os princípios fundamentais do PbD.

Em Sphere Identity (2018) são especificados fatores que os desenvolvedores devem considerar ao implementar sistemas que estejam em conformidade com o GDPR. Também é relatado o que é necessário para garantir a privacidade em todo o processo de desenvolvimento de software. Entretanto, não menciona como aplicar os princípios do PbD.

Deleersnyder (2018) reforça que o GDPR torna o PbD um requisito legal na União Europeia e ilustra o ciclo de vida de desenvolvimento seguro para planejar,

projetar, construir, testar e entregar sistemas de informações focados em segurança. Embora cite o PbD, não menciona como os seus princípios são aplicados ao ciclo de vida apresentado.

Por fim, Staats (2023) discute como os requisitos de privacidade, como mensagens de informações de coleta de dados, avisos de utilização de *cookies*, entre outros, são abordados em *websites* e visualizados pelo usuário final. Não há qualquer menção de como implementar estes requisitos em um processo de desenvolvimento de software ou um guia que auxilie os engenheiros de software a identificá-los.

4.5 Considerações sobre o Capítulo

Os estudos encontrados na RSL contribuíram para o avanço da aproximação do PbD com a Engenharia de Software, porém, ainda é necessário compreender como os princípios do PbD podem ser implementados como atividades práticas na Engenharia de Software, principalmente no contexto de processos ágeis de desenvolvimento, mencionados apenas em dois estudos. Entretanto, em ambos os estudos, não é fornecido um método, processo ou diretriz para apoiar as atividades de Engenharia de Software, foco do presente trabalho de pesquisa.

CAPÍTULO 5 - ESTUDO DE CASO

Este capítulo apresenta os estudos de caso realizados com o intuito de compreender como a privacidade de dados pessoais está sendo integrada ao processo de desenvolvimento de software nas organizações, especialmente aquelas que estão sob a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018a).

A estrutura e a estratégia desta pesquisa estão posicionadas no âmbito do projeto de pesquisa intitulado: *Privacy by Design Plug-in*: um *plugin* de processo de software para integração da privacidade de dados pessoais no desenvolvimento ágil de software. Este projeto foi aprovado pelo Comitê de Ética em Pesquisa (CEP) da Pontifícia Universidade Católica do Paraná (PUCPR) sob Parecer Nº 5.629.309. Por motivos de confidencialidade, os nomes das organizações e colaboradores entrevistados foram anonimizados, omitidos ou generalizados para garantir a confidencialidade das informações coletadas que serão utilizadas unicamente para fins de pesquisa.

Os documentos relacionados ao projeto de pesquisa estão disponíveis nos Apêndices: A.1 - Carta de Apresentação; A.2 - Termo de Compromisso e Utilização dos Dados (TCUD); A.3 - Termo de Consentimento Livre e Esclarecido (TCLE); e A.5 - Carta de Autorização da Instituição. Por causa da natureza desta pesquisa e para evitar a exposição à COVID-19, todos os participantes assinaram digitalmente os documentos.

Este capítulo está organizado da seguinte maneira. A Seção 5.1 descreve o protocolo de pesquisa utilizado na condução do estudo de caso. A Seção 5.2 discute os resultados obtidos. A Seção 5.3 apresenta as conclusões do estudo. Por fim, a Seção 5.4 relata as considerações do capítulo.

5.1 Protocolo do Estudo de Caso

Para compreender como a privacidade dos dados pessoais está sendo integrada ao processo de desenvolvimento de software, optou-se pelo método de estudo de caso, com coleta de dados por meio de dez entrevistas semiestruturadas

com membros de equipes de desenvolvimento de software de cinco organizações. Como a pesquisa abrange mais de uma organização de desenvolvimento de software, é definido como um estudo de caso múltiplo, adaptando o método proposto por Yin (2018), conforme ilustrado na Figura 7.

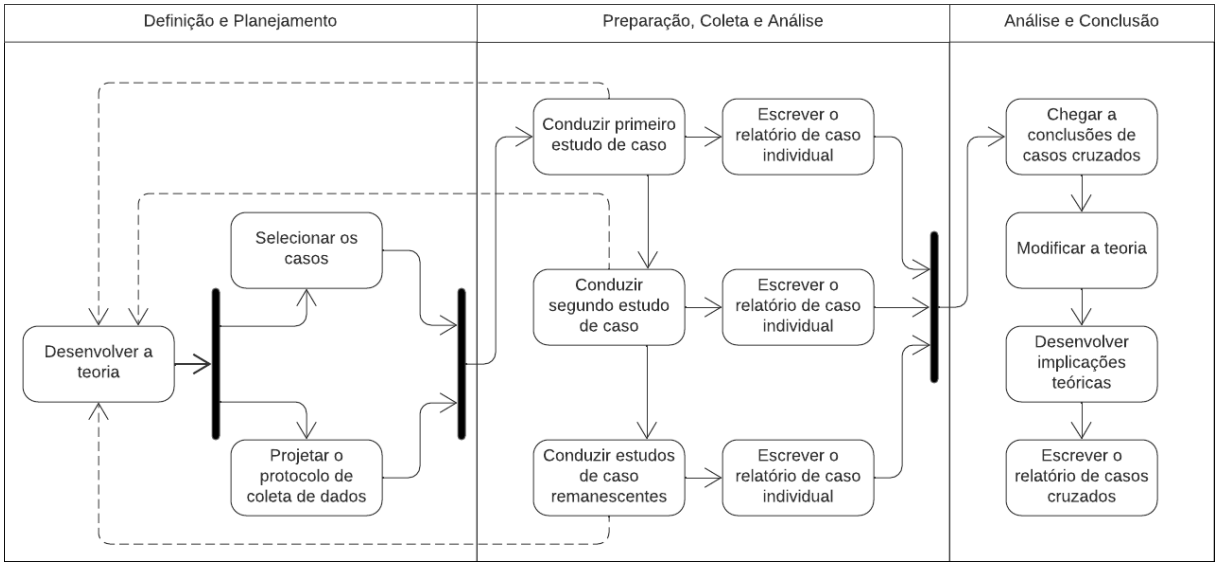

Figura 7. Método de Estudo de Caso. Adaptado de Yin (2018).

A etapa inicial, nomeada de Definição e Planejamento possui as atividades: (i) desenvolver a teoria; (ii) selecionar os casos; e (iii) projetar o protocolo de coleta de dados. Esta etapa afetará as etapas seguintes, pois é neste momento que o pesquisador realiza toda a preparação e organização da pesquisa.

Na próxima etapa, Preparação, Coleta e Análise, ocorre a execução do estudo de caso. As atividades presentes são: (i) conduzir o estudo de caso escolhido; e (ii) escrever o relatório de caso individual. Segundo Rainer e Hall (2002), pode-se repetir iterativamente esta etapa até que todas as possibilidades sejam esgotadas e que novos estudos de caso não colaborem na evolução da pesquisa. Para a execução desta etapa, um convite foi enviado via e-mail à cada colaborador.

Por fim, a etapa de Análise e Conclusão obtém as seguintes atividades: (i) chegar a conclusões de casos cruzados; (ii) modificar a teoria; (iii) desenvolver implicações teóricas; e (iv) escrever o relatório dos casos cruzados.

5.1.1 Questões de Pesquisa e Proposições

O estudo de caso visava responder as seguintes questões:

1. **Como a privacidade de dados pessoais está sendo integrada ao desenvolvimento ágil de software?**
2. **Quais são as dificuldades associadas a esta integração?**

Com o intuito de responder às questões de pesquisa, elaborou-se as Proposições (P) com base em questões retiradas da literatura, apresentadas na sequência:

P1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.

Os seguintes conceitos de suporte foram utilizados para a composição da estrutura da Proposição P1:

i. Dificuldade na adoção dos princípios fundamentais do *Privacy by Design* (PbD) (CAVOUKIAN, 2009a, 2012a);
ii. Integração dos princípios do PbD em processos de desenvolvimento (RYGGE; JØSANG, 2018; VIITANIEMI, 2017);
iii. Dificuldades enfrentadas pelos desenvolvedores ao incorporar a privacidade de dados no design de software (SENARATH; ARACHCHILAGE, 2018).
iv. Ausência de práticas explícitas para requisitos não funcionais em processos de desenvolvimento (CURCIO *et al.*, 2018);
v. Manifesto Ágil (CUNNINGHAM, 2001).

Em (CAVOUKIAN, 2009a, 2012a), Cavoukian apresenta os 7 (sete) princípios fundamentais do *Privacy by Design* que visam implementar medidas a assegurar a privacidade de dados pessoais de maneira proativa. Nestes estudos são mencionadas as dificuldades em aplicar os princípios em todas as etapas de desenvolvimento, desde a concepção do projeto até a sua conclusão.

Os estudos de Viitaniemi (2017) e Rygge e Josang (2018) apresentam propostas para a implementação dos princípios do PbD no desenvolvimento ágil de software. Enquanto o primeiro propõe três etapas a serem executadas em conjunto com as atividades do *framework* Scrum, o segundo propõe um jogo a estimular os desenvolvedores a considerar requisitos não funcionais, como privacidade e segurança, na identificação dos requisitos funcionais do projeto.

Senarath e Arachchilage (2018) investigam como os desenvolvedores incorporam a privacidade nos designs de software e quais os problemas enfrentados. Como descobertas deste estudo, revelou-se que há carência de conhecimento por parte dos desenvolvedores em como aplicar corretamente o conceito de privacidade de dados.

Os fatores que dificultam a implementação de requisitos não funcionais, como por exemplo, privacidade de dados, segurança, usabilidade, entre outros, em processos ágeis, são explorados no estudo de Curcio *et al.* (2018).

Por fim, o Manifesto Ágil estabelece doze princípios que enfatizam as equipes, entrega frequente de software, colaboração do cliente, respostas eficazes às mudanças, melhoria contínua, equipes autogeridas e avaliações internas. Desde então, diversas metodologias ágeis tornaram-se populares, como Scrum (SCHWABER; SUTHERLAND, 2020), eXtreme Programming (XP) (BECK, 2000), Lean (POPPENDIECK; POPPENDIECK, 2003), Kanban (ANDERSON, 2010), entre outras.

P2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.

Os seguintes conceitos de suporte foram utilizados para a composição da estrutura da Proposição P2:

i. Modelagem de processos de negócios em conformidade legal (ARAÚJO *et al.*, 2021).
ii. Dificuldades enfrentadas pelos desenvolvedores ao incorporar a privacidade de dados no design de software (SENARATH; ARACHCHILAGE, 2018), de forma semelhante ao utilizado na Proposição P1.

iii. Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a);
iv. *General Data Protection Regulation* (GDPR) (EU, 2016);
v. Especificação da terminologia comum de privacidade e recomendações sobre dados pessoais (ISO/IEC 27701, 2019; ISO/IEC 29100, 2011).

Em Araújo *et al.* (2021) são discutidas as razões pelas quais as organizações ainda não estão em conformidade com os novos procedimentos legais, mesmo a LGPD estando em vigor desde setembro de 2020. Neste estudo ainda são relatados alguns padrões, como consentimento, direito de acesso, transferência internacional de dados, entre outros, que auxiliam os analistas a modelar os processos de negócio da organização para atingir conformidade com a LGPD.

A Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a) estabelece como deve ocorrer o tratamento de dados pessoais em território brasileiro, incluindo os meios digitais, por pessoa pública ou jurídica sendo de direito público ou privado. De forma semelhante, o *General Data Protection Regulation* (GDPR) (EU, 2016) tem como objetivo, dentre outros, contribuir com a proteção de dados pessoais dos cidadãos europeus.

No âmbito das normas técnicas, a ISO/IEC 29100:2011 especifica uma terminologia comum de privacidade, além da definição dos papéis dos atores no processo para garantir a proteção de informações de identificação pessoal em sistemas de informação. Por fim, a ISO/IEC 27701:2019 propõe recomendações específicas sobre dados pessoais e estabelece orientações para implementar, manter e melhorar um sistema de gerenciamento de privacidade no contexto de uma organização.

5.1.2 Unidades de Análise

A seleção das organizações para participar dos estudos de caso seguem os seguintes critérios:

- Organização de desenvolvimento de software situada no Brasil que utiliza metodologias ágeis de desenvolvimento de software;
- Independentemente de ser utilizada uma subcontratação, a organização deve exercer o controle sobre o ciclo de vida do desenvolvimento de software.

5.1.3 Recrutamento

Por meio da mídia social corporativa LinkedIn[34], enviou-se o convite diretamente aos profissionais identificados como amostra do estudo que deveriam atuar ou gerenciar *squads* de desenvolvimento de software nas organizações.

Dez profissionais de cinco organizações responderam afirmando que concordavam em participar da pesquisa. Então, os seguintes documentos foram enviados via e-mail:

- Carta de Apresentação: apresenta o pesquisador e os objetivos da pesquisa aos participantes, visando a obtenção da autorização para a realização do estudo. Este documento encontra-se no Apêndice A.1;
- Termo de Compromisso e Utilização de Dados (TCUD): por meio deste documento o pesquisador se compromete a não apresentar de forma individual qualquer informação coletada, garantindo assim o sigilo das informações e a não identificação das organizações, fornecendo, desta maneira, segurança aos respondentes da pesquisa. Este documento encontra-se no Apêndice A.2;
- Termo de Consentimento Livre e Esclarecido (TCLE): garante a ética e a integridade na pesquisa, assegurando que os participantes estejam plenamente cientes e de acordo com sua participação, contribuindo para a proteção dos direitos e bem-estar dos envolvidos. Este documento encontra-se no Apêndice A.3;
- Carta de Autorização da Instituição: concede permissão/autorização para realizar pesquisas e/ou estudos com colaboradores da instituição. Neste documento estão descridas as informações específicas sobre a natureza e o propósito da atividade, bem como as condições ou restrições associadas a ela. A carta de autorização encontra-se no Apêndice A.5;
- Elaboração do Instrumento de Pesquisa: questionário elaborado a partir dos objetivos e questões propostas no documento de visão geral da pesquisa. O questionário encontra-se na Seção 5.1.4.

[34] Site LinkedIn: https://www.linkedin.com/

A documentação enviada foi lida e assinada pelo profissional, concordando em participar do estudo. Neste mesmo e-mail, foi solicitado ao participante que indicasse o melhor data e horário para a entrevista, que não deveria ultrapassar 60 (sessenta) minutos. As entrevistas foram realizadas virtualmente intermediadas pelo serviço de comunicação Google Meet[35].

5.1.4 Pontos de Análises

Os Pontos de Análises (PA) têm como objetivo estruturar todas as questões que um determinado assunto contempla, para que, durante a entrevista, tópicos importantes não sejam esquecidos por parte do entrevistador, o que poderia levar a necessidade de uma nova intervenção junto à organização.

Cada ponto de análise possui número de identificação, descrição do ponto de análise, descrição detalhada dos pontos de análises para fundamentar a entrevista, e proposição(ões) relacionada(s). O Quadro 5 apresenta um modelo da descrição de cada ponto de análise.

Quadro 5. Modelo de Descrição dos Pontos de Análises.

Ponto de Análise nº: descrição dos pontos de análises.	
Descrição detalhada dos pontos de análises para fundamentar as questões do estudo de caso. *Citações diretas mencionadas pelos entrevistados.*	Proposições relacionadas

Seguindo o modelo do Quadro 5, definiram-se os seguintes pontos de análises, ilustrados no Quadro 6.

Quadro 6. Descrições dos Pontos de Análises.

Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	
(i) a organização possui algum processo estabelecido para o desenvolvimento de software? (ii) há processos específicos utilizados na organização para a integração da privacidade de dados pessoais em projetos ágeis? (iii) como esses processos são realizados?	P1

[35] Site Google Meet: https://meet.google.com/

(iv) quais artefatos são gerados como resultados desses processos específicos para a integração da privacidade de dados pessoais em projetos ágeis? (v) em que medida a organização leva em consideração a privacidade de dados pessoais ao longo do ciclo de vida do dado (coleta, armazenamento, acesso, compartilhamento e eliminação)?	
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	
(i) há alguma iniciativa da organização para a alocação de especialistas em privacidade de dados pessoais na formação dos times de desenvolvimento ágil? (ii) como os especialistas em privacidade de dados pessoais são envolvidos nos projetos de desenvolvimento de software? (iii) os especialistas em privacidade de dados pessoais trabalham nos mesmos times de desenvolvimento dos produtos de software ou são alocados separadamente sob demanda?	P1
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	
(i) há alguma iniciativa na organização para a promoção do conhecimento na área de privacidade de dados pessoais? (ii) a equipe técnica foi treinada para ter conhecimento na área de privacidade de dados pessoais? (iii) a organização possui uma política que fomente o treinamento na área de privacidade de dados pessoais? (iv) a organização reserva recurso organizacional para investimento em treinamento do corpo técnico na área de privacidade de dados pessoais? (v) a organização reserva recurso organizacional para investimento em treinamento do corpo técnico na área de desenvolvimento ágil?	P1
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	
(i) há alguma ferramenta utilizada pelo time de desenvolvimento que auxilie a integração da privacidade de dados pessoais ao desenvolvimento do produto de software? (ii) quais são as ferramentas e em que fase do projeto elas são utilizadas? (iii) de que forma essas ferramentas auxiliam o desenvolvimento do produto de software?	P1
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	
(i) como a alta gerência da organização apoia a criação e a implantação de políticas que fomentam a integração do desenvolvimento ágil de software e a privacidade de dados pessoais? (ii) que valor a alta gerência enxerga que a privacidade de dados pessoais agrega ao produto de software? (iii) a entrega de software funcional em um curto espaço de tempo é priorizada em detrimento da privacidade de dados pessoais?	P2

(iv)	como ocorre a priorização das demandas?	
(v)	no processo de desenvolvimento da organização existe uma fase específica para o levantamento e reconhecimento de todos os usuários que utilizarão o sistema?	
(vi)	como os usuários do sistema são envolvidos no processo de desenvolvimento?	
(vii)	a opinião desses usuários afeta a forma como o sistema é desenvolvido?	

5.1.5 Relacionamento dos Pontos de Análises com Proposições

Com o intuito de sintetizar os resultados de cada ponto de análise, utilizaram-se os seguintes formatos:

- ● - o ponto de análise **foi encontrado** na organização;
- ◐ - o ponto de análise **foi encontrado parcialmente** na organização;
- ○ - o ponto de análise **não foi encontrado** na organização;

Cada proposição, definida na Subseção 5.1.4, é verificada na organização. Para demonstrar a avaliação de capa proposição adotaram-se as seguintes classificações:

- ● - a proposição foi considerada **verdadeira**;
- ◐ - a proposição foi considerada **parcialmente verdadeira**;
- ○ - a proposição foi considerada **não verdadeira**;

5.1.6 Análise dos Dados

As entrevistas foram transcritas e os materiais codificados pelos procedimentos de análise qualitativa (STRAUSS; CORBIN, 1998). Para este estudo, utilizou-se a Codificação Aberta (SALDAÑA, 2013) por meio da ferramenta ATLAS.ti[36], versão 9. Os dados foram interpretados e rotulados com base em suas propriedades e contexto. Dessa forma, dois ou mais dados relacionados ao mesmo assunto foram marcados com o mesmo código, mesmo em entrevistas diferentes.

[36] Site ATLAS.ti: https://atlasti.com/

A primeira interação envolveu a codificação das entrevistas. Os dados obtidos foram divididos em segmentos a partir dos quais foram criados os códigos iniciais. A codificação foi então analisada e o resultado serviu como base de conhecimento para a codificação das demais entrevistas.

Segundo Saldaña (2013), a Codificação Axial e Seletiva representa o segundo ciclo de codificação. Para realizar a Codificação Axial, analisaram-se os códigos criados para identificar semelhanças existentes para que pudessem ser agregados de acordo com contexto, causalidade e consequências. Identificadas as semelhanças, os códigos foram agrupados em categorias.

5.2 Resultados e Discussões

Após a realização das entrevistas e a finalização da Codificação Aberta, Axial e Seletiva, foi possível gerar todas as práticas identificadas nas organizações. Os códigos que emergiram das entrevistas foram organizados nas categorias: Processo de Desenvolvimento de Software, identificados na cor cinza; Times de Desenvolvimento de Software, apresentados na cor verde; Conhecimento da Equipe Técnica, ilustrados na cor amarela; e Políticas Organizacionais, definidos na cor ciano.

Em Processos de Desenvolvimento de Software estão relacionados os códigos: Existência de Processo de Desenvolvimento de Software, Cerimônias do Processo de Desenvolvimento de Software, Utilização de Ferramentas na Integração de Privacidade de Dados Pessoais, e Participação do Cliente na Tomada de Decisão sobre Coleta de Dados Pessoais.

Na categoria Times de Desenvolvimento de Software encontram-se os códigos: Iniciativa de Alocação de Especialista em Privacidade de Dados Pessoais, Equipe Responsável por Questões Relacionadas à Privacidade de Dados Pessoais, e Composição dos Times.

A categoria Conhecimento da Equipe Técnica é formada pelos códigos: Treinamento dos Colaboradores na Área de Privacidade de Dados, Troca de Informações sobre Privacidade de Dados, e Confusão entre os Conceitos de “Segurança” e “Privacidade”.

Por fim, a categoria Políticas Organizacionais está relacionada aos códigos: Privacidade de Dados Pessoais como Valor ao Produto de Software, Reserva de Recurso para Treinamento em Privacidade de Dados Pessoais, Políticas que Fomentam a Integração da Privacidade de Dados ao Desenvolvimento de Software, e Priorização de Demandas em Detrimento a Privacidade de Dados Pessoais.

Os detalhes das entrevistas de cada organização encontram-se no Apêndice D. A Figura 8 apresenta a rede gerada pela própria ferramenta ATLAS.ti na fase de Codificação Seletiva, que apresenta, de maneira visual, as relações entre os diferentes códigos identificados durante a análise de dados qualitativos.

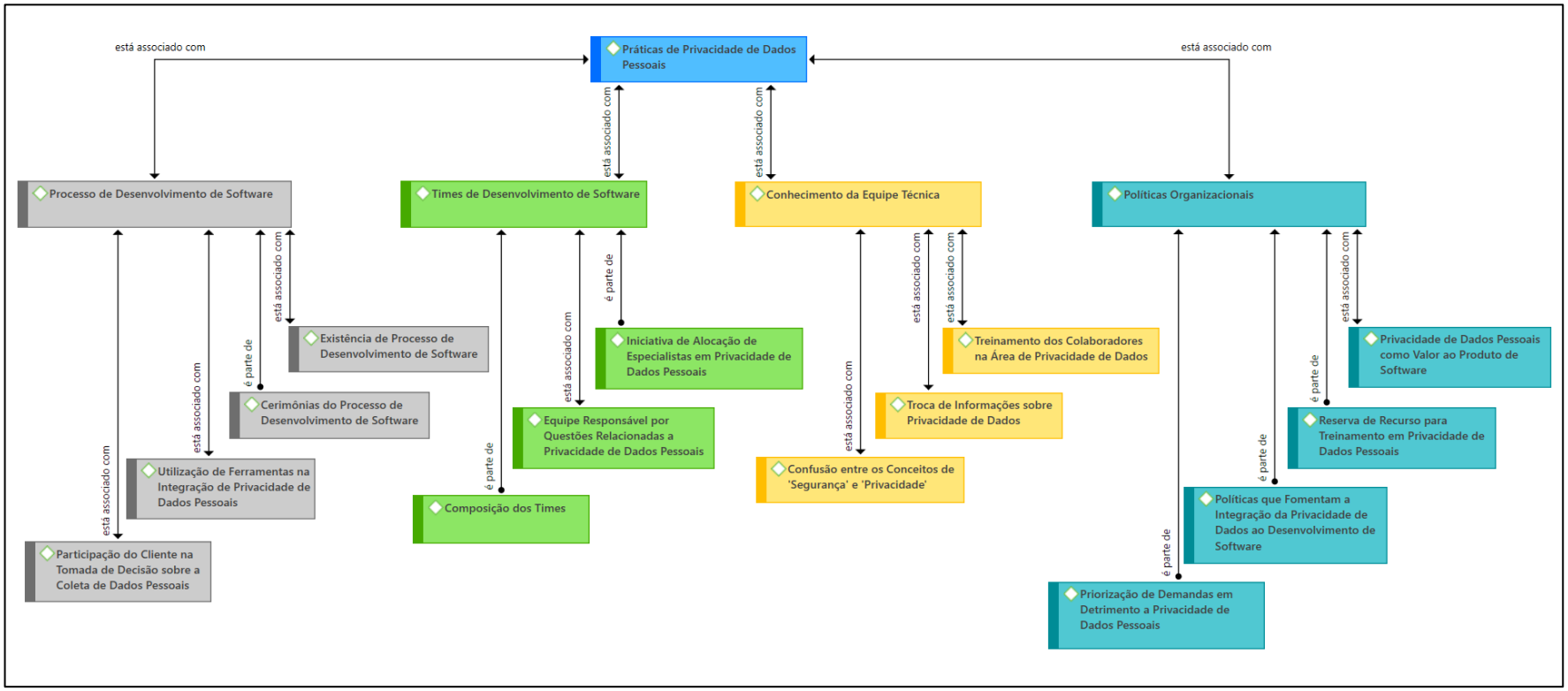

Figura 8. Rede Gerada na Fase de Codificação.

O Quadro 7 apresenta um resumo comparativo dos pontos de análise entre as organizações entrevistadas.

Quadro 7. Visão Geral do Resultado dos Pontos de Análise.

Organização	Pontos de Análise				
	PA-01	PA-02	PA-03	PA-04	PA-05
A	○	○	◐	○	○
B	○	○	◐	○	◐
C	◐	○	●	○	○
D	○	○	○	○	●
E	◐	○	◐	●	●

De acordo com o Ponto de Análise 01 (PA-01), em nenhuma organização foi possível verificar a plena integração da privacidade dos dados pessoais no processo de software. Somente as organizações C e E possuem cuidados específicos com a privacidade dos dados pessoais. Enquanto na Organização C existe uma política que revisa anualmente o que foi desenvolvido para identificar e solucionar vulnerabilidades relacionadas à privacidade de dados pessoais. Na Organização E, um comitê é responsável por verificar a conformidade legal do produto desenvolvido. Neste ponto de análise, seria importante que as organizações integrassem as preocupações de privacidade e proteção de dados pessoais em todo o ciclo de vida de desenvolvimento de software, e não apenas nas fases posteriores de implementação.

Para que as organizações se preocupem com as questões de privacidade de dados desde as etapas iniciais do projeto, as equipes devem integrar profissionais com profundo conhecimento de privacidade e proteção de dados pessoais para resolver problemas durante o ciclo de desenvolvimento do produto, e não apenas realizar uma revisão por uma equipe independente após o produto estar implementado.

Embora as equipes não possuam um profissional dedicado e com expertise em privacidade de dados pessoais (PA-02), constatou-se que as organizações oferecem cursos de capacitação sobre esse tema para seus colaboradores (PA-03). Em algumas organizações, os profissionais devem realizar esses cursos no momento da

contratação. Em outras organizações, os profissionais podem realizar cursos em momentos específicos para atualizar e aprimorar suas competências. Porém, constatou-se que se trata de cursos introdutórios sobre privacidade de dados pessoais, LGPD (BRASIL, 2018a), vulnerabilidades, entre outros temas, e não têm como objetivo a formação de especialistas na área. Neste cenário, sugere-se que ao menos um membro da equipe realize cursos periódicos de privacidade e proteção de dados pessoais. Dessa forma, cada equipe poderia ter um especialista que pudesse disseminar o conhecimento aos demais integrantes do seu time.

O uso de ferramentas que auxiliam na integração da privacidade de dados no desenvolvimento de software, PA-04, foi encontrado apenas na Organização D, que utiliza um software para atendimento à LGPD (BRASIL, 2018a) e ao GDPR (EU, 2016), e uma segunda ferramenta para prestar atendimento aos seus clientes, dando-lhes transparência e autonomia sobre os dados pessoais armazenados. Outras organizações não se preocupam com questões de privacidade de dados nem realizam processos de verificação de vulnerabilidades manualmente. É importante ressaltar que os colaboradores utilizam o termo “segurança” para se referir à “privacidade”, sem fazer distinção entre os termos. Neste ponto de análise, diversos softwares foram mencionados pelos colaboradores. No entanto, tratava-se especificamente de software de segurança da informação.

Por fim, o Ponto de Análise 05 (PA-05) não foi encontrado em duas Organizações, A e C. Embora estas organizações tenham questões relacionadas à privacidade de dados, elas possuem uma política de atendimento aos requisitos da legislação, incluindo a privacidade de dados pessoais. Além disso, as Organizações A e C estão reestruturando as suas equipes para que a privacidade dos dados seja cada vez mais integrada ao processo de desenvolvimento. As Organizações D e E possuem equipes específicas para analisar a conformidade legal do produto desenvolvido. Portanto, a alta gestão das organizações não pretende integrar a privacidade e a proteção de dados pessoais durante o ciclo de desenvolvimento do produto.

Após realizar os estudos de caso com as organizações, o Quadro 8 apresenta um resumo das análises de cada proposição considerando os resultados obtidos por meio das entrevistas semiestruturadas.

Quadro 8. Visão Geral dos Resultados das Análises das Proposições.

Proposição	Organização					Resultado Final
	A	B	C	D	E	
P1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●	●	●	●	●	●
P2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	○	◐	○	●	●	◐

A **Proposição 1 foi considerada verdadeira**, pois ao analisá-la individualmente em cada organização, encontraram-se evidências que em todas as organizações, apesar de possuírem um modelo ágil de desenvolvimento de software, este não integra, de maneira sistemática, atividades relacionadas à privacidade de dados pessoais. Apenas na Organização E há uma etapa dedicada a investigar vulnerabilidades relacionadas a privacidade de dados. Porém, esta atividade ocorre após a entrega de valor pelo time de desenvolvimento.

Em relação aos times de desenvolvimento e conhecimento em privacidade de dados pessoais pelo corpo técnico da organização, encontrou-se unanimidade nas organizações analisadas. As equipes são formadas por profissionais multidisciplinares, entretanto, não há na sua composição um especialista em privacidade de dados pessoais. Constatou-se que em apenas duas Organizações (D e E) o produto de software é submetido a auditorias. Na primeira, isso ocorre por meio de uma organização terceira que verifica, identifica e documenta as inconformidades legais dos produtos de software. Na segunda, há na própria organização uma equipe que atua juntamente ao departamento jurídico na verificação de adequação legal do produto desenvolvido.

A **Proposição 2 foi considerada parcialmente verdadeira**, pois não foram encontradas evidências que comprovam a dificuldade em reformular seus processos em busca da conformidade com as leis e regulamentos. Constatou-se que a alta gerência das organizações analisadas reconhece a importância do seu produto contemplar requisitos de privacidade, bem como estar em conformidade legal.

Neste sentido, verificou-se que a Organização A está reestruturando sua equipe técnica e seus processos em busca de solucionar problemas relacionados à LGPD. Entretanto, constatou-se que as Organizações D e E possuem políticas para integrar a privacidade de dados em seus processos de desenvolvimento de software. Além disso, identificou-se que, em alguns casos, a Organização E prioriza a entrega de software funcional em detrimento a entrega dos produtos no prazo estabelecido, mesmo que isso signifique não contemplar corretamente os requisitos não funcionais, como privacidade de dados pessoais.

5.3 Considerações sobre o Estudo de Caso

Foram entrevistados dez profissionais de desenvolvimento de software com experiência de 8 a 23 anos em cinco organizações de tamanhos variados, empregando de 100 a mais de 10.000 pessoas cada. As organizações operam em diversos setores, incluindo varejo, serviços financeiros, fábrica de software e desenvolvimento de hardware.

Embora as organizações expressem preocupações sobre a conformidade legal e a qualidade do software devido aos possíveis riscos para a sua reputação decorrentes de violações de dados, o estudo revela que equipes específicas ou terceiros abordam frequentemente a privacidade dos dados em uma fase posterior de desenvolvimento. Isso contradiz leis como LGPD e GDPR, que enfatizam o atendimento aos requisitos de privacidade de dados pessoais durante todo o ciclo de desenvolvimento do produto.

Observou-se que as equipes de desenvolvimento de software das organizações entrevistadas não possuem especialistas em privacidade de dados. Além disso, não incentivam seus colaboradores a realizarem cursos e treinamentos aprofundados sobre o assunto, causando falta de conhecimento. Além disso, os entrevistados não fazem distinção entre os termos “privacidade” e “segurança”. Quando questionados, relataram que os desafios de privacidade e segurança são tratados da mesma forma na organização.

Como perspectivas de trabalho futuro, pretende-se replicar o estudo em organizações de diferentes dimensões, com sedes em outros países e domínios, para verificar como as questões relacionadas com a privacidade de dados pessoais estão sendo integradas no processo de desenvolvimento de software.

5.4 Considerações sobre o Capítulo

Este capítulo apresentou o estudo de caso realizado por meio de dez entrevistas semiestruturadas com membros de equipes de desenvolvimento de software de cinco organizações para compreender como a privacidade dos dados pessoais está sendo integrada ao processo de desenvolvimento de software das organizações e quais são as dificuldades enfrentadas para realizar esta integração.

A pesquisa indicou que as organizações entrevistadas tratam a questão da privacidade de dados pessoais em etapas posteriores ao desenvolvimento de software. Isso vai de encontro às legislações, como a LGPD e o GDPR, que destacam a importância de atender aos requisitos de privacidade de dados pessoais ao longo de todo o ciclo de desenvolvimento do produto. Consequentemente, é necessário estabelecer um processo de desenvolvimento de software para auxiliar as organizações, independente de porte e domínio, a integrar a privacidade dos dados pessoais e estar em conformidade com as legislações vigentes.

CAPÍTULO 6 - PROCESSO DE DESENVOLVIMENTO DE SOFTWARE ORIENTADO À PRIVACIDADE (PDSOP)

Este capítulo apresenta o Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP), além do papel do guardião da privacidade e dos artefatos propostos com base na realização das atividades da *Design Science Research Methodology* (DSRM). A Seção 6.1 destaca o PDSOP e o papel do Guardião de Privacidade. A Seção 6.2 descreve os artefatos propostos. A Seção 6.3 exibe a integração do PDSOP no desenvolvimento de software. A Seção 6.4 aborda a o repositório de informações. Por fim, a Seção 6.5 discorre sobre as considerações do capítulo.

6.1 Caracterização do PDSOP

O processo proposto, denominado PDSOP, visa integrar a privacidade de dados pessoais dos titulares ao desenvolvimento de software, independentemente no modelo de processo utilizado pelas organizações, como por exemplo, Scrum (SCHWABER; SUTHERLAND, 2020), Kanban (ANDERSON; CARMICHAEL, 2016), entre outros. Para possibilitar tal integração são definidos novos artefatos, perfil e práticas específicas. A Figura 9 apresenta o PDSOP.

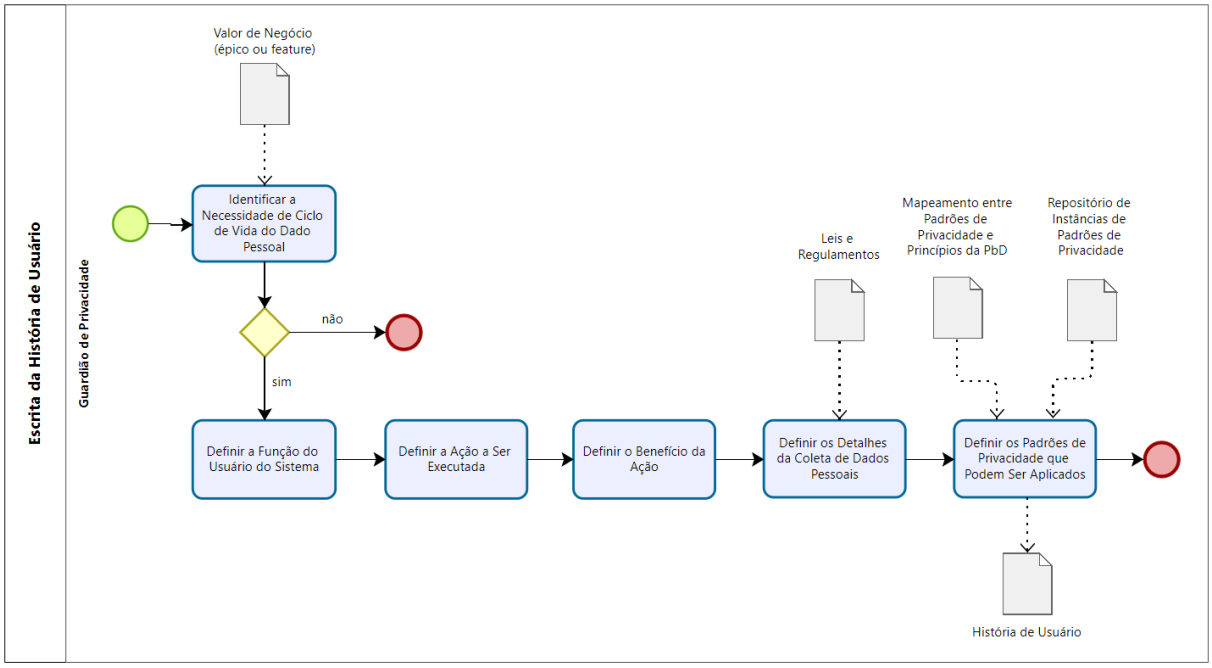

Figura 9. Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP).

Ao fim da execução das atividades contidas no processo tem-se a escrita de histórias de usuário, adaptando o modelo Connextra (COHN, 2004), conforme detalhado na Seção 2.1. Ao todo, o PDSOP possui seis atividades, as quais serão detalhadas nas Subseções 6.1.1 a 6.1.6. Porém, antes deste detalhamento é necessário apresentar o papel “Guardião de Privacidade”, que é o responsável por executar as atividades e promover valores relacionados à proteção de dados pessoais desde o início do projeto de desenvolvimento de software.

GUARDIÃO DE PRIVACIDADE

Definição do Papel

O Guardião de Privacidade atua como ponto focal de questões relacionadas à proteção de dados pessoais no seu time de desenvolvimento. Este profissional deve estar em constante comunicação com o departamento jurídico e com o *Data Protection Officer* (DPO) da organização a fim de se atualizar sobre leis, regulamentos e tecnologias que impactam diretamente em seus projetos de software. Além de participar de treinamentos e eventos externos relacionados à proteção de dados pessoais e privacidade de modo geral.

Perfil Esperado

Espera-se que o profissional responsável possua as seguintes características, habilidades e qualificações:

- Conhecimento Técnico: deve compreender como as tecnologias podem afetar a privacidade dos usuários;
- Conhecimento de Leis e Regulamentos: deve compreender as leis e regulamentos relacionados à privacidade e proteção de dados pessoais, principalmente aquelas aplicáveis à região em que atua;
- Comunicação Eficaz: deve ser capaz de repassar seus conhecimentos de maneira clara e concisa aos demais membros do time de desenvolvimento que atua;
- Pensamento Crítico: deve ser capaz de avaliar riscos e tomar decisões informadas sobre como proteger a privacidade dos usuários;
- Trabalho em Equipe: deve ser capaz de trabalhar em equipe e colaborar com os demais membros do time de desenvolvimento de software para garantir que a privacidade seja considerada desde o início do processo de desenvolvimento;
- Adaptabilidade: deve ser capaz de se adaptar às mudanças em regulamentações e tecnologias da informação e estar sempre atualizado com as novidades na área de proteção de dados pessoais.

Responsabilidades

O Guardião de Privacidade é o profissional responsável pelas questões relacionadas à privacidade de dados pessoais no seu time de desenvolvimento. Portanto, é seu dever executar as seguintes atividades do PDSOP:

- Identificar a Necessidade de Ciclo de Vida do Dado Pessoal;
- Definir a Função do Usuário do Sistema;
- Definir a Ação a ser Executada;
- Definir o Benefício da Ação;
- Definir os Detalhes da Coleta de Dados Pessoais;
- Definir os Padrões de Privacidade que Podem Ser Aplicados.

Atuação na Organização

O Guardião de Privacidade possui a responsabilidade de defender e difundir o conhecimento adquirido aos membros do time de desenvolvimento do qual faz parte, por meio de treinamentos e *workshops*. Isso permite que todos compreendam a importância de manter os projetos em conformidade legal evitando riscos desnecessários à organização, além de prevenir futuros retrabalhos por parte da equipe.

Uma vez que os membros do time de desenvolvimento possuem conhecimento e conscientização sobre a importância da implementação de requisitos de privacidade de dados, em caso da ausência do Guardião de Privacidade por motivos de saúde, férias ou capacitação profissional, os demais membros do time terão condições de assumir temporariamente as tarefas do colaborador ausente, garantindo a continuidade do trabalho e minimizando o impacto nos projetos em andamento.

Além disso, o Guardião de Privacidade deve alinhar as atividades, responder questões, elucidar dúvidas e auxiliar na resolução de vulnerabilidades e problemas enfrentados pela equipe, garantindo que os requisitos relacionados à privacidade de dados pessoais sejam implementados ao longo do ciclo de vida do projeto.

No âmbito organizacional, o Guardião de Privacidade pode, com sua experiência, propor melhorias e ferramentas no processo de desenvolvimento, realizar treinamentos relacionados à privacidade de dados pessoais com os novos colaboradores da organização e capacitar novos guardiões de privacidade. Idealmente, cada time de desenvolvimento deve ser composto por, ao menos, um Guardião de Privacidade. Contudo, não há necessidade de ser um novo profissional dedicado exclusivamente a esta função. As responsabilidades deste papel podem ser incorporadas à colaboradores existentes na composição dos times de desenvolvimento, como por exemplo, Analista de Qualidade, Arquiteto de Soluções ou Líder Técnico.

Treinamentos Recomendados

É de interesse e responsabilidade da organização garantir que o Guardião de Privacidade esteja em constante atualização para desempenhar eficazmente suas funções relacionadas à proteção de dados e privacidade, uma vez que qualquer problema relacionado à privacidade de dados recairá sobre a organização. Como treinamentos, recomenda-se:

- Princípios do *Privacy by Design*;
- Regulamentações de privacidade e proteção de dados em vigor que incidam nos projetos de desenvolvimento;
- Certificações de privacidade e proteção de dados.

Benefícios e Pontos de Atenção

Entre os principais benefícios em se ter Guardiões de Privacidade integrando os times de desenvolvimento, pode-se citar:

- Foco em Privacidade de Dados Pessoais: o Guardião de Privacidade é um profissional especialista em proteção de dados, o que contribui com a equipe na identificação e correção de potenciais vulnerabilidades e ameaças do tema durante o ciclo de desenvolvimento, garantindo que as boas práticas de privacidade não sejam negligenciadas;
- Conscientização na Equipe: o Guardião de Privacidade atua como defensor da privacidade de dados, promovendo a conscientização sobre questões de privacidade na equipe de desenvolvimento. Isso pode gerar uma forte cultura de privacidade nos times que possuam este papel;
- Identificação Proativa de Vulnerabilidades: o Guardião de Privacidade atua de maneira proativa na identificação de vulnerabilidades de privacidade durante todo o desenvolvimento do projeto, conforme mencionam os princípios do *Privacy by Design* (CAVOUKIAN, 2009a);
- Conformidade com Leis e Regulamentos: o Guardião de Privacidade deve estar atualizado com as legislações vigentes nas regiões em que atua, o que reduz significativamente os riscos de a organização não estar em conformidade legal.

É importante ressaltar alguns pontos de atenção com a atribuição do papel de Guardião de Privacidade atuando nos times de desenvolvimento:

- Carga Adicional: conforme mencionado, o Guardião de Privacidade é um papel que poderá ser assumido por um colaborador que possui outras responsabilidades. Isso pode sobrecarregar este profissional e prejudicar seu desempenho em suas funções;

- Comunicação Ineficaz: se não houver uma comunicação eficaz entre o Guardião de Privacidade e os demais membros do time de desenvolvimento, os conhecimentos de privacidade de dados pessoais podem não ser adequadamente compartilhados, resultando em lacunas na compreensão e aplicação das práticas de privacidade;
- Dependência de um Indivíduo: a dependência exclusiva de um Guardião de Privacidade para questões de privacidade de dados pode criar um único ponto de falha. Caso este profissional se ausente, pode haver uma lacuna nos assuntos de sua responsabilidade;
- Custo Adicional de Treinamento: investir em treinamento de um Guardião de Privacidade pode representar um custo adicional para a organização.

Para mitigar estes pontos de atenção, sugere-se que o papel de Guardião de Privacidade seja absorvido por profissionais com interesse e aptidão ao tema. Além disso, formar novos Guardiões no próprio time de desenvolvimento pode ser uma estratégia, a fim de dividir as responsabilidades com outros membros da equipe, minimizando a dependência de um único profissional.

Em relação à comunicação com o time de desenvolvimento, pode-se estabelecer canais de comunicação para discutir regularmente questões de privacidade de dados, sempre mantendo os demais membros do time atualizados ao tema e ao andamento do projeto.

Por fim, os custos de treinamentos dos colaboradores devem ser tratados como parte do desenvolvimento contínuo da equipe, uma vez que, se a organização enfrentar problemas judiciais relacionados à privacidade de dados pessoais, os valores relacionados às multas podem exceder os investimentos na atualização de seus colaboradores.

Diferença entre o papel do Guardião de Privacidade e a função *Data Protection Officer* (DPO)

Algumas legislações e regulamentos vigentes em diversos países, como o GDPR (EU, 2016) e a LGPD (BRASIL, 2018a), determinam que as organizações devem designar um profissional que será responsável por assegurar que a empresa está em conformidade com as leis vigentes na região em que atuam. Esta função

recebe o nome de *Data Protection Officer* (DPO) no GDPR e Encarregado na LGPD. Ambos os profissionais possuem a responsabilidade fazer a intermediação entre os titulares dos dados e os agentes de tratamento, como aceitar reclamações, prestar esclarecimentos e adotar providências. Além disso, é de obrigação do DPO/Encarregado responder às autoridades nacionais em nome da organização em que atua, além de adotar providências para adequar a organização às leis e regulamentos vigentes relacionados à privacidade e proteção de dados pessoais.

Por outro lado, o Guardião de Privacidade é o líder técnico do time de desenvolvimento em que atua, auxiliando a equipe na conscientização, treinamento e desenvolvimento de procedimentos relacionados à privacidade e proteção de dados pessoais. Perante as leis e regulamentos, o Guardião de Privacidade não possui uma função formal que responde em nome da organização.

A seguir são detalhadas as atividades do PDSOP, que têm como responsável o Guardião de Privacidade.

6.1.1 Identificar a Necessidade de Ciclo de Vida do Dado Pessoal

Propósito

A atividade tem como objetivo avaliar se um determinado valor de negócio faz uso de dados pessoais, fornecendo uma resposta objetiva sobre a necessidade ou não desses dados no contexto da operação.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade;

Product Owner;

Stakeholders.

Entradas

Valor de Negócio (Épico ou *Feature*).

Tarefas Executadas

1. Análise do Valor de Negócio: o Guardião de Privacidade analisa minuciosamente o valor de negócio fornecido para compreender as funcionalidades e objetivos associados;
2. Identificação de Dados Pessoais: identifica se o valor de negócio faz uso de dados pessoais. Isso envolve a identificação de informações que possam ser diretamente associadas a indivíduos;
3. Avaliação de Necessidade de Dados Pessoais: o Guardião de Privacidade determina se o valor de negócio requer o tratamento de dados pessoais para atender aos objetivos específicos.

Saídas

Relatório de Necessidade de Dados Pessoais[37]: a saída desta atividade é um relatório objetivo indicando se há ou não necessidade de dados pessoais para a implementação do valor de negócio.

6.1.2 Definir a Função do Usuário do Sistema

Propósito

Identificar e compreender os atores envolvidos em um requisito específico, assim como determinar quem será beneficiado pela funcionalidade resultante. Isso contribui para uma compreensão abrangente dos *stakeholders* e seus impactos no sistema.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade;

Product Owner;

Stakeholders.

[37] Relatório de Necessidade de Dados Pessoais: Como sugestão de relatório, pode-se realizar a Avaliação do Impacto na Proteção de Dados (DPIA, em inglês *Data Protection Impact Assessment*) sobre a proteção de dados pessoais, conforme mencionado por Freitas (2022).

Entradas

Valor de Negócio (Épico ou *Feature*).

Tarefas Executadas

1. Identificação de Atores Envolvidos: o Guardião de Privacidade e o Product Owner identificam e listam todos os atores que têm um papel direto ou indireto no requisito em análise. Isso pode incluir usuários finais, membros da equipe, sistemas externos ou outras entidades relevantes;
2. Análise de Beneficiados: uma análise é realizada para determinar quem será beneficiado pela funcionalidade resultante do requisito. Isso pode incluir usuários do software, a própria organização, sistemas externos ou outros *stakeholders*.

Saídas

Relatório de Atores e Beneficiados: a saída desta atividade é um relatório identificando os atores envolvidos associados ao requisito específico.

6.1.3 Definir a Ação a Ser Executada

Propósito

Determinar as ações específicas que o sistema deve executar em suporte aos usuários identificados durante a atividade “Definir a Função do Usuário do Sistema”. A atividade “Definir a Ação a Ser Executada” visa traduzir os requisitos e expectativas dos usuários em ações concretas a serem realizadas pelo sistema.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade;

Product Owner;

Stakeholders.

Entradas

Relatório de Atores e Beneficiados.

Tarefas Executadas

1. Análise de Requisitos do Usuário: o Guardião de Privacidade e o Product Owner analisam os requisitos e expectativas dos usuários identificados na atividade anterior, considerando suas necessidades específicas;
2. Tradução em Ações do Sistema: com base na análise, são definidas as ações específicas que o sistema deve executar para atender aos requisitos dos usuários. Isso inclui funcionalidades, interações, interfaces e quaisquer outras operações relevantes;
3. Validação com os Stakeholders: as ações propostas são validadas com os stakeholders, para garantir que as expectativas estejam alinhadas e que não haja lacunas na compreensão.

Saídas

Relatório de Ações do Sistema: a saída desta atividade é um relatório especificando as ações que o sistema deve executar em suporte aos usuários identificados.

6.1.4 Definir o Benefício da Ação

Propósito

Fornecer uma justificativa clara e detalhada para as ações definidas para o usuário, concentrando-se nos objetivos que serão alcançados e nos problemas que a funcionalidade proposta resolverá. Visa estabelecer um entendimento claro do valor agregado ao atender às necessidades do usuário.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade;

Product Owner;

Stakeholders.

Entradas

Relatório de Ações do Sistema.

Tarefas Executadas

1. Identificação dos Objetivos: o Guardião de Privacidade e o Product Owner identificam e documentam os objetivos que serão alcançados ao implementar as ações definidas para o usuário;
2. Análise dos Problemas Resolvidos: uma análise aprofundada é realizada para compreender os problemas específicos que a funcionalidade proposta resolverá. Isso pode incluir lacunas no processo atual, desafios enfrentados pelos usuários ou deficiências em funcionalidades existentes;
3. Justificativa para a Necessidade do Usuário: o Guardião de Privacidade e o Product Owner articulam porque o usuário precisa da funcionalidade, destacando os benefícios diretos que serão alcançados. Isso pode envolver melhorias na eficiência, redução de erros, aumento da satisfação do usuário, entre outros.

Saídas

Relatório de Benefícios da Ação do Usuário: a saída desta atividade é um relatório que descreve resumidamente os benefícios associados à ação proposta para o usuário.

6.1.5 Definir os Detalhes da Coleta de Dados Pessoais

Propósito

Identificar quais dados pessoais serão coletados no contexto do sistema, avaliando a natureza sensível ou não desses dados. Além disso, determina o tempo

de retenção desses dados e analisa as restrições legais específicas que impactam o ciclo de vida do dado, considerando as leis e regulamentos aplicáveis em cada país.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade.

Entradas

Relatório de Benefícios da Ação do Usuário;

Leis e Regulamentos.

Tarefas Executadas

1. Identificação de Dados Pessoais: analisar os requisitos do sistema e identificar quais dados pessoais serão manipulados;
2. Avaliação de Sensibilidade dos Dados: determinar a natureza sensível ou não dos dados pessoais identificados, considerando o impacto potencial para os indivíduos caso esses dados sejam comprometidos;
3. Definição do Tempo de Retenção: estabelecer o tempo de retenção para os dados pessoais, levando em consideração requisitos legais, regulatórios e de necessidade operacional;
4. Análise das Restrições Legais: analisar as leis e regulamentos específicos de privacidade de dados em cada país relevante, identificando as restrições legais que afetam o ciclo de vida do dado pessoal coletado.

Saídas

Documento de Análise de Dados Pessoais e Legislação: a saída desta atividade é um documento detalhado que descreve quais dados pessoais serão coletados, a sensibilidade desses dados, o tempo de retenção e as restrições legais aplicáveis.

6.1.6 Definir os Padrões de Privacidade que Podem Ser Aplicados

Propósito

Definir os padrões de privacidade que serão adotados durante a implementação da ação, garantindo que as práticas de coleta, retenção, processamento, armazenamento, compartilhamento ou eliminação de dados pessoais estejam alinhadas com as normas e regulamentos específicos de privacidade de dados pessoais.

Papel Responsável

Guardião de Privacidade.

Papéis Envolvidos

Guardião de Privacidade.

Entradas

Documento de Análise de Dados Pessoais e Legislação.

Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design*;

Repositório de Instâncias de Padrões de Privacidade.

Tarefas Executadas

1. Análise dos Requisitos de Privacidade: analisar os requisitos específicos de privacidade derivados da análise de dados pessoais e das leis aplicáveis, identificando as necessidades específicas que devem ser abordadas pelos padrões de privacidade.
2. Seleção de Padrões de Privacidade: com base na análise, selecionar os padrões de privacidade mais adequados para a implementação da ação. Para isso, os artefatos “Mapeamento entre Padrões de Privacidade e Princípios do PbD” (detalhado na Subseção 6.2.2) e “Repositório de Instâncias de Padrões de Privacidade” (detalhado na Subseção 6.2.3), podem ser acessados por meio do Repositório de Informações (Seção 6.4) que tem como objetivo auxiliar o time de desenvolvimento na adoção da melhor estratégia para a resolução do problema.

Saídas

História de Usuário: descrição de uma funcionalidade ou recurso do software, contendo a função do usuário do sistema, ação a ser executada, benefício da ação, dados pessoais coletados (sensíveis ou não), tempo de retenção, leis e/ou regulamentos seguidos, restrições e recomendações de padrões de privacidade.

O artefato de saída proposto, História de Usuário, é apresentado na Figura 10, Seção 6.2.1.

6.2 Artefatos Propostos

Nesta Seção são abordados os três artefatos definidos no PDSOP (Figura 9). A Subseção 6.2.1 detalha a História de Usuário, artefato gerado a partir da execução das atividades do processo. A Subseção 6.2.2 descreve o artefato “Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design*”. Por fim, a Subseção 6.2.3 exibe o artefato denominado “Repositório de Instâncias de Padrões de Privacidade”.

6.2.1 História de Usuário

Para exemplificar a especificação de requisitos utilizando o PDSOP, pode-se citar o contexto de comércio eletrônico. Neste cenário, o usuário realizará uma compra de um determinado produto. Para isto, é necessário coletar dados como nome completo do usuário, gênero, e-mail, data de nascimento, endereço para entrega e informações de pagamento.

Considerando o PDSOP (Figura 9), na primeira atividade, denominada “Identificar a Necessidade de Ciclo de Vida do Dado Pessoal”, o Guardião de Privacidade identifica que haverá coleta e armazenamento de dados pessoais para o desenvolvimento desde valor de negócio.

Na próxima atividade, “Definir a Função do Usuário do Sistema”, é identificado o ator que fará uso da ação. Neste caso, o ator é um usuário do comércio eletrônico. A ação realizada pelo ator, definida na atividade “Definir Ação a Ser Executada”, é de comprar um produto disponível no comércio eletrônico. O benefício da funcionalidade, estabelecido na atividade “Definir o Benefício da Ação”, é usufruir das facilidades de pesquisa e economia de tempo e dinheiro, uma vez que o usuário não precisará sair de sua residência para efetuar a compra e receber o produto.

Na atividade seguinte, “Definir os Detalhes da Coleta de Dados Pessoais”, são estabelecidos quais dados pessoais do titular são necessários. Neste exemplo, pode-se citar o nome completo do usuário, e-mail, data de nascimento, endereço para entrega e informações de pagamento, além de dados sensíveis, como gênero.

Nesta mesma atividade, o Guardião de Privacidade que está escrevendo a história de usuário deve se atentar as leis e regulamentos que incidem sobre o tratamento de dados pessoais, como por exemplo, a Lei Geral de Proteção de Dados Pessoais (LGPD) quando a operação de tratamento de dados for realizada no território nacional (BRASIL, 2018a).

Entretanto, a LGPD não determina o período de tratamento de dados, sendo necessário verificar quais dados pessoais serão coletados e qual a finalidade específica do tratamento. Por exemplo, para dados referentes ao sistema tributário nacional, incide a Lei Nº 5.172, de 25 de Outubro de 1966, que determina em seu Artigo 174, que a ação para a cobrança do crédito tributário prescreve em 5 (cinco) anos (BRASIL, 1966). Por outro lado, prontuários de pacientes devem ser armazenados por 20 (vinte) anos, conforme estabelece a Lei Nº 13.787, de 27 de Dezembro de 2018 (BRASIL, 2018b). Sendo assim, cabe ao Guardião de Privacidade identificar a finalidade do tratamento de dados para determinar o tempo de retenção dos dados pessoais. No cenário do comércio eletrônico, utiliza-se as Leis nº 13.709 e nº 5.172, devido às informações de pagamento.

Como restrições de privacidade de dados pessoais, o usuário deve receber informações claras e concisas sobre a coleta, armazenamento e compartilhamento de seus dados pessoais e a coleta só pode ocorrer mediante o consentimento informado por ele.

Por fim, na atividade “Definir os Padrões de Privacidade que podem ser Aplicados” o Guardião de Privacidade pode recomendar o uso de padrões de privacidade os quais podem ser aplicados a fim de prover uma solução adequada à ação que será implementada pelo time de desenvolvimento de software. O Repositório de Informações, descrito na Seção 6.4, tem como objetivo auxiliá-lo na busca e escolha dos padrões.

No cenário do comércio eletrônico, os padrões de privacidade Privacy Policy Display e Obtaining Explicit Consent podem ser recomendados. Enquanto o primeiro menciona como deve ser a apresentação da política de privacidade e como os dados

pessoais serão coletados e tratados, o segundo possui o foco na obtenção do consentimento do titular dos dados.

Ao final do processo, o artefato História de Usuário é gerado. A Figura 10 ilustra a história de usuário escrita considerando todas as informações originadas das macro etapas de refinamento de requisitos e de definição dos critérios de aceite de privacidade de dados pessoais.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero adquirir um produto pelo comércio eletrônico.
Para que eu possa economizar tempo e dinheiro com deslocamento.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo
- E-mail
- Data de Nascimento
- Endereço
- Informações de Pagamento</td><td>Dados Pessoais Sensíveis:
- Gênero</td><td>Tempo de Retenção:
5 anos</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Os usuários devem receber informações claras e concisas sobre quais dados pessoais serão coletados.
- Os usuários devem receber informações sobre o compartilhamento dos seus dados pessoais.
- Os usuários devem consentir com o uso dos seus dados pessoais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Policy Display;
- Obtaining Explicit Consent.</td></tr>
</table>

Figura 10. Artefato História de Usuário Gerado a partir do PDSOP.

Após a elaboração de uma história de usuário, é fundamental reconhecer que a responsabilidade pela priorização não é especificamente definida pelo PDSOP, mas sim delegada ao processo utilizado pela organização. Diversas metodologias ágeis, como Scrum e Kanban, oferecem estruturas eficazes para a gestão do *Product Backlog*, incluindo a tarefa de priorização.

A delegação dessa responsabilidade para o processo organizacional garante flexibilidade, permitindo que a equipe se alinhe aos princípios e práticas que melhor se adéquem ao contexto específico da organização. Isso também possibilita a adaptação à dinâmica e às necessidades em constante evolução do time e do projeto.

Ao adotar essa abordagem, alinha-se a premissa de que as organizações têm a liberdade de escolher e ajustar suas práticas de acordo com os requisitos

específicos, as características da equipe e as demandas do projeto. Dessa forma, as histórias de usuário, após sua criação, são integradas ao *Product Backlog* e, subsequentemente, priorizadas dentro do contexto do método escolhido pela organização para melhor atender aos objetivos estratégicos e às necessidades do negócio.

6.2.2 Mapeamento entre Padrões de Privacidade e Princípios do PbD

Conforme mencionado em capítulos anteriores, engenheiros de software e times de desenvolvimento carecem de guias, métodos, modelos e *frameworks* que os auxiliem a aplicar os princípios do *Privacy by Design* (PbD) no desenvolvimento de software. Porém, a aplicação na prática destes princípios ainda é um desafio a ser superado, pois são considerados de alto nível de abstração para serem aplicados em projetos de desenvolvimento de software (ALSHAMMARI; SIMPSON, 2017a; BUGEJA; JACOBSSON, 2020; GALVEZ; GURSES, 2018).

Entretanto, os padrões de privacidade fornecem conhecimento e soluções estruturadas, documentadas e reutilizáveis que, ao serem aplicadas corretamente, apoiam no desenvolvimento de softwares seguros, confiáveis e com foco na privacidade de dados pessoais. Portanto, são soluções menos abstratas quando comparadas aos princípios do PbD (COLESKY; HOEPMAN; HILLEN, 2016; LENHARD; FRITSCH; HEROLD, 2017).

Com o objetivo de aproximar os princípios do PbD com as atividades práticas da Engenharia de Software, realizou-se um mapeamento entre os 72 (setenta e dois) padrões de privacidade catalogados pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024) e os 7 (sete) Princípios do PbD (CAVOUKIAN, 2009a). O mapeamento contou, além do autor da presente pesquisa, com dois docentes da área de informática que auxiliaram no processo do mapeamento a fim de evitar viés por parte do pesquisador.

Cada participante recebeu um guia contendo a introdução ao conceito e princípios do PbD (CAVOUKIAN, 2009a) e a descrição da introdução aos padrões de privacidade contendo contexto, problema abordado e solução proposta (UC BERKELEY SCHOOL OF INFORMATION, 2024). Como treinamento, os três participantes realizaram juntos o mapeamento do padrão de privacidade Location Granularity, discutindo o porquê de o padrão contemplar ou não um determinado

princípio do PbD. Após mapear o primeiro padrão, cada participante realizou individualmente o mapeamento dos demais padrões. Ao todo, o processo ocorreu em três etapas: treinamento; mapeamento preliminar contendo outros seis padrões de privacidade; e mapeamento dos demais 65 padrões de privacidade divididos em cinco sessões de 13 padrões cada. Entre as sessões, reuniões eram realizadas para se obter os resultados dos mapeamentos de todos os participantes e, para as relações em que havia divergências, discussões eram realizadas com o intuito de obter consenso entre todos os participantes. Ao fim de cada reunião novos padrões de privacidade eram selecionados para a próxima sessão de mapeamento.

Para garantir a confiança do mapeamento, foi estabelecida a confiabilidade entre os participantes. O Coeficiente de Correlação Intraclasse (ICC) tem sido amplamente utilizado para medir a confiabilidade ou o grau de semelhança entre os avaliadores. O ICC é equivalente o Coeficiente Kappa para variáveis contínuas: também varia entre 0 e 1 e pode ser interpretado da seguinte forma: ICC < 0,4 é fraco; 0,4 ≤ CCI < 0,75 é satisfatório a bom; ICC ≥ 0,75 é excelente (FLEISS; LEVIN; PAIK, 2013).

Com o intuito de verificar a concordância entre os participantes ao realizar a avaliação, calculou-se a concordância 2 a 2:

- Participante A e Participante B: 81,55%, índice de concordância excelente;
- Participante A e Participante C: 86,31%, índice de concordância excelente;
- Participante B e Participante C: 79,37%, índice de concordância excelente.

Os mapeamentos realizados por cada participante, encontram-se em sua totalidade no Apêndice E. O resultado do mapeamento entre os Padrões de Privacidade e os Princípios do PbD são apresentados nos Quadros 9, 55 e 56, organizados de acordo com a(s) Estratégia(s) de Hoepman (2014). As linhas que apresentam o caractere (●) indicam que o Padrão de Privacidade em questão contempla o princípio do PbD respectivo à coluna. Por outro lado, sua ausência indica a não relação.

No Quadro 9 encontram-se os Padrões de Privacidade relacionados às estratégias *Abstract* e *Control*. Os Padrões de Privacidade relacionados as demais estratégias são apresentadas nos Quadros 55 e 56 (Apêndice F).

Quadro 9. Resultado do Mapeamento entre Padrões de Privacidade e Princípios do PbD relacionados às estratégias Abstract e Control.

Estratégia de Hoepman (2014)	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Abstract	Location Granularity	●	●	●				●
Control	Decoupling [content] and location information visibility	●	●	●				●
Control	Active broadcast of presence		●				●	●
Control	Buddy List				●			●
Control	Discouraging blanket strategies	●		●				●
Control	Enable/Disable Functions			●			●	●
Hide Control	Encryption with user-managed keys	●	●	●		●		
Control	Incentivized Participation		●					●
Inform Control	Informed Consent for Web-based Transactions						●	●
Control	Lawful Consent	●		●			●	●
Control	Masquerade			●		●		●
Control	Negotiation of Privacy Policy	●	●					●
Control	Outsourcing [with consent]	●					●	
Control	Pay Back			●				●
Control	Obtaining Explicit Consent						●	●
Separate Control	Personal Data Store			●		●	●	●
Control	Private link		●	●				
Control	Reasonable Level of Control	●		●				●
Control	Reciprocity			●			●	●
Control	Selective access control		●	●				●
Control	Selective Disclosure	●	●	●				●
Control	Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context						●	●
Control	Single Point of Contact	●		●		●		●

Com foco na coleta de dados relacionada à localização de um usuário, o padrão Location Granularity visa, de maneira proativa, prevenir que os dados de localização do titular não sejam compartilhados sem seu consentimento. Para isso, o objetivo do padrão é minimizar a coleta de informações oferecendo níveis diferentes de granularidade e oferecer ao titular dos dados a opção do quão preciso gostaria de compartilhar a sua localização. Com isso, o padrão Location Granularity abarca os

princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Relacionado ao padrão Location Granularity, o padrão Decoupling [Content] and Location Information Visibility permite ao usuário decidir sobre o compartilhamento, divulgação e granularidade de suas informações relacionadas à localização a fim de utilizar um determinado serviço. Caso nenhuma configuração seja realizada por parte do usuário, o sistema deve, por padrão, preservar a privacidade dos dados pessoais do usuário proativamente. Desta forma, o padrão Decoupling [Content] and Location Information Visibility compreende os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

O padrão Active Broadcast of Presence permite que o usuário opte quando compartilhar suas informações, impedindo que os dados sejam transmitidos de maneira holística em qualquer situação e, em caso de dúvidas, esclarecimentos devem ser fornecidos a ele. É possível que o usuário opte por não ser questionado novamente, porém esta decisão deve ser realizada de maneira explícita. Neste contexto, o padrão Active Broadcast of Presence contempla os princípios Privacidade por Padrão, Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

No contexto de redes sociais, frequentemente os usuários interagem não apenas com pessoas próximas, mas também com desconhecidas. O padrão Buddy List possibilita ao usuário manter listas de contatos de relevância com as quais possui maior probabilidade de interagir. Sendo assim, o padrão Buddy List está diretamente relacionado aos princípios Funcionalidade Total e Respeito pela Privacidade do Usuário.

Ainda no contexto de compartilhamento de informações e redes sociais, o padrão Discouraging Blanket Strategies concede aos usuários o controle total sobre a privacidade do conteúdo que está sendo compartilhado, possibilitando-os definir o nível de privacidade que melhor se adequa às suas necessidades. Com isso, o padrão Discouraging Blanket Strategies abrange os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Para que o padrão Enable/Disable Functions tenha êxito em sua aplicação, deve-se, de modo antecipado, ter conhecimento sobre quais funcionalidades o sistema possui e quais informações pessoais são coletadas em cada uma destas

funções, permitindo que o titular concorde ou não com a coleta de determinadas informações. Deste modo, os princípios Privacidade Incorporada ao Design, Visibilidade e Transparência e Respeito pela Privacidade do Usuário são contemplados pelo padrão Enable/Disable Functions.

A fim de garantir a segurança e a privacidade dos dados pessoais dos titulares, o padrão Encryption With User-Managed Keys tem como intuito criptografar as informações pessoais dos titulares antes de armazená-las ou transferi-las por meio de serviços online. Com isso, os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Segurança de Ponta a Ponta são considerados no padrão Encryption With User-Managed Keys.

A participação dos usuários em um determinado sistema fornecendo dados pessoais, a fim de melhorar a identificação de suas preferências é uma necessidade dos controladores de dados. Neste contexto, o padrão Incentivized Participation incentiva a participação dos usuários sem que prejudique ou invada a privacidade dos titulares. Qualquer atividade que necessite coletar dados do usuário, o consentimento prévio deve ser informado. Portanto, o padrão Incentivized Participation está relacionado aos princípios Privacidade por Padrão e Respeito pela Privacidade do Usuário.

Para manter um serviço rentável, além de fornecer uma melhor experiência ao usuário, os controladores necessitam coletar dados pessoais dos titulares. Entretanto, a coleta só é permitida mediante o consentimento informado pelo titular de dados. Com isso, o padrão de privacidade Informed Consent for Web-based Transactions visa proteger os interesses dos titulares dos dados e estabelece que a coleta de informações pessoais só pode ocorrer mediante o seu consentimento, e esta só poderá ocorrer após a apresentação de informações claras e concisas sobre como os dados serão coletados, armazenados, processados e excluídos. Sendo assim, o padrão Informed Consent for Web-based Transactions engloba os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Neste mesmo contexto de obtenção de consentimento dos titulares de dados, o padrão Lawful Consent estabelece que os serviços devem ser separados e, para cada serviço específico, um consentimento explícito deve ser adquirido prevenindo que o usuário compartilhe seus dados pessoais sem o conhecimento prévio de uma determinada funcionalidade. Desta maneira, os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design, Visibilidade e

Transparência e Respeito pela Privacidade do Usuário são contemplados no padrão Lawful Consent.

O padrão Masquerade tem como objetivo permitir ao usuário selecionar o nível de compartilhamento de informações pessoais para um determinado contexto. Isso é realizado por meio da organização das informações pessoais em escalas de privacidade. Quando o usuário seleciona um nível na escala, todas as informações daquele e de níveis inferiores são compartilhadas. Neste contexto, o padrão Masquerade inclui os princípios Privacidade Incorporada ao Design, Segurança de Ponta a Ponta e Respeito pela Privacidade do Usuário.

O padrão Negotiation of Privacy Policy propõe que as preferências de privacidade destes usuários, quando não reconhecidas, sejam configuradas sempre preservando ao máximo a sua privacidade. Este cuidado deve ocorrer incorporando desde o início do uso do serviço, técnicas que permitam a proteção da privacidade do usuário. Isso é feito pela implantação de uma restrição de vazamento de dados até que o usuário determine quais informações podem ser compartilhadas, respeitando assim, sua privacidade. Neste contexto, o padrão Negotiation of Privacy Policy envolve os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão e Respeito pela Privacidade do Usuário.

Em alguns casos, os controladores necessitam compartilhar os dados com terceiros a fim destes realizarem o processamento dos dados do titular. O padrão Outsourcing [with consent] estabelece que, para estes casos, os controladores devem apresentar de maneira transparente aos titulares, quais são os dados e como eles serão processados por terceiros. O processamento destes dados por terceiros só será permitido após a obtenção do consentimento livre, específico e explícito do titular dos dados. Desse modo, o padrão Outsourcing [with consent] contempla os princípios Proativo não Reativo; Prevenir não Remediar e Visibilidade e Transparência.

O padrão Pay Back fornece benefícios aos usuários quando realizam contribuições ou mantêm conteúdo para o serviço, como em uma rede social. Porém, deve-se respeitar as escolhas individuais dos usuários e, para aqueles que optarem por conceder mais informações, deve-se obter o consentimento legal do titular. Com isso, o padrão Pay Back está relacionado aos princípios Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

O padrão Obtaining Explicit Consent visa fornecer ao titular dos dados notificações claras e objetivas informando-o como um determinado serviço coletará,

processará e armazenará seus dados. O controlador deve garantir que o titular compreenda as informações e consequências de aceitar os termos apresentados. O consentimento por parte do titular deve ser dado livremente. Portanto, o padrão Obtaining Explicit Consent compreende os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

A combinação de um servidor central e *tokens* pessoais é discutida no padrão Personal Data Store. Neste padrão, os *tokens* podem assumir chaves USB e incorporam um sistema de banco de dados e um certificado de autenticação para o titular. Com isso, os titulares possuem maior controle de seus dados pessoais que permanecem seguros e armazenados localmente e passíveis de manutenções pelo próprio titular. Sendo assim, o padrão Personal Data Store contempla os princípios Privacidade Incorporada ao Design, Segurança de Ponta a Ponta, Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

O padrão Private Link tem como objetivo fornecer ao titular um link privado para um recurso específico, como por exemplo, um conjunto de informações pessoais do usuário. Se julgar necessário, o titular pode compartilhar o link com outras pessoas, dando-lhes acesso àquelas informações pessoais. Com isso, o padrão Private Link engloba os princípios Privacidade por Padrão e Privacidade Incorporada ao Design.

A fim de permitir que os usuários forneçam informações de maneira seletiva e granular, o padrão Reasonable Level of Control visa, de maneira antecipada, projetar meios de possibilitar ao titular escolher o nível de privacidade de seus dados, concedendo a terceiros, acesso a essas informações. Neste contexto, o padrão Reasonable Level of Control está relacionado aos princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Em sistemas que os usuários devem colaborar entre si a favor do grupo, a qualidade do resultado é dada por meio da contribuição de todos os membros. O padrão Reciprocity menciona que cada membro deve ser recompensado proporcionalmente a sua participação perante os ganhos do grupo. Qualquer coleta e utilização dos dados dos usuários deve ser consentida e informado como esses dados pessoais serão utilizados, respeitando a sua privacidade. Desse modo, o padrão Reciprocity inclui os princípios Privacidade Incorporada ao Design, Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

O padrão Selective Access Control fornece aos usuários o controle da visibilidade do conteúdo compartilhado em ambiente sociais. Os usuários podem especificar regras com base em outros usuários ou grupos de pessoas para definir para quem destinará a postagem. Com isso, o padrão Selective Access Control compreende os princípios Privacidade por Padrão, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Em algumas ocasiões os usuários desejam utilizar de maneira anônima um serviço minimizando assim as chances de fornecerem seus dados pessoais. Em contrapartida, os controladores necessitam de algumas informações, pois, desta maneira, os usuários não poderão realizar atividades maliciosas sem que sejam identificados. Para estes casos, o padrão Selective Disclosure identifica quais informações são essenciais para o funcionamento do sistema, promovendo assim a minimização de dados. Além disso, funcionalidades anônimas devem ser fornecidas ao usuário, desde que não comprometa o serviço. Portanto, os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário são considerados pelo padrão Selective Disclosure.

Para que haja o processamento dos dados pessoais dos usuários, o controlador necessita do consentimento dos titulares. Neste contexto, o padrão Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context estabelece que o serviço deve apresentar ao usuário mecanismos por meio dos quais os dados serão coletados e como serão processados, além de vincular ao controlador ou aos seus representantes. Estas informações devem ser apresentadas de maneira clara e objetiva e a coleta de dados só poderá ser realizada após a obtenção do consentimento do usuário. Dessa maneira, o padrão Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context abarca os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Os serviços de armazenamento distribuído exigem gerenciamento de privacidade especializado. O padrão Single Point of Contact adota uma abordagem por meio do fornecimento de *tokens* de segurança para autenticar e autorizar a apresentação de informações confidenciais a um determinado usuário, além do armazenamento de pseudônimos a fim de preservar a identidade do titular dos dados. Sendo assim, o padrão Single Point of Contact compreende os princípios Proativo não

Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design, Segurança de Ponta a Ponta e Respeito pela Privacidade do Usuário.

Os demais Padrões de Privacidade associados às estratégias *Separate*, *Hide*, *Minimize*, *Enforce e Inform* encontram-se no Apêndice F.

Com o mapeamento entre os Padrões de Privacidade e os Princípios do PbD, constata-se uma complexidade para correlacioná-los, pois, por vezes, a natureza abstrata dos princípios do PbD gera dúvidas ao relacioná-los ao Padrão de Privacidade. Posteriormente, estas dúvidas foram sanadas em reuniões com os demais participantes, nas quais houve uma explanação para se chegar a um consenso naquela correlação específica entre um determinado Padrão de Privacidade e um princípio específico do PbD.

Além disso, observa-se uma similaridade conceitual entre os Padrões de Privacidade e os princípios do PbD, vinculando-se, então, a prática com a teoria. Como resultado do mapeamento, obtém-se um instrumento que foi integrado ao PDSOP, cuja finalidade é de auxiliar engenheiros de software na tomada de decisão e implementação de problemas específicos de privacidade considerando os princípios do PbD exigidos pelas legislações e regulamentos.

6.2.3 Repositório de Instâncias de Padrões de Privacidade

O catálogo dos 72 (setenta e dois) Padrões de Privacidade destinados a orientar práticas seguras no desenvolvimento de software, em sua forma original, frequentemente apresentam-se vagas e teóricas, o que dificulta o seu entendimento por parte dos profissionais de desenvolvimento de software.

O artefato “Repositório de Instâncias de Padrões de Privacidade” surge como uma resposta a essa necessidade, o qual busca preencher a lacuna entre a teoria e a prática ao fornecer exemplos concretos de aplicação dos padrões de privacidade no cotidiano dos times de desenvolvimento de software. Esta iniciativa almeja não apenas simplificar a compreensão desses padrões, mas também capacitar profissionais a incorporá-los de maneira significativa em seus projetos.

O repositório adota uma abordagem prática, apresentando os padrões catalogados em casos aplicáveis, enriquecidos por contexto, identificação de problemas recorrentes e apresentação de soluções por meio da escrita de histórias de usuário, conforme artefato proposto na Subseção 6.2.1. O objetivo deste artefato

é catalisar uma maior assimilação dos Padrões de Privacidade por parte de desenvolvedores, sobretudo Guardiões de Privacidade, fomentando a aplicação eficaz desses padrões em seus respectivos domínios de atuação.

A expectativa é que esse repositório não apenas simplifique a compreensão dos Padrões de Privacidade, mas também encoraje sua adoção sistemática em projetos de desenvolvimento de software por fornecer uma compilação substancial de exemplos práticos. Sendo assim, espera-se um maior fortalecimento da conscientização sobre privacidade por parte dos desenvolvedores, além de promover a implementação dos padrões que são essenciais para a construção de ambientes digitais seguros e eticamente responsáveis.

Conforme mencionado na Seção 6.2.1, a Lei Geral de Proteção de Dados Pessoais (LGPD (BRASIL, 2018a) não determina o período de tratamento de dados, sendo necessário analisar quais dados pessoais serão coletados, além dos dados necessários para a finalidade específica do tratamento. Entretanto, para ilustrar os cenários apresentados nesta subseção, adotou-se o tempo de cinco anos de retenção das informações pessoais.

Location Granularity

Maria é usuária de um aplicativo de viagens que fornece informações e opiniões de conteúdos relacionados ao turismo. Para uma melhor experiência, o aplicativo coleta informações pessoais do usuário, como nome completo, e-mail, geolocalização, preferências de viagens, avaliações e opiniões de locais visitados. Entretanto, Maria está preocupada em fornecer tantos dados pessoais, pois ela utiliza o aplicativo apenas para receber sugestões de locais turísticos nas cidades que visita. Por este motivo, ela gostaria de escolher o nível de precisão de sua localização, visto que para utilizar a funcionalidade de sugestões do aplicativo não é necessário que o software colete a localização precisa do usuário, como por exemplo, apenas a cidade que Maria está, seria suficiente.

Para este cenário, o padrão de privacidade Location Granularity pode ser utilizado, pois permite ao usuário escolher o nível de precisão de sua localização, como por exemplo, localização precisa, moderada ou aproximada. A Figura 11 apresenta a história de usuário para o cenário descrito.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero receber sugestões de locais turísticos na cidade que estou visitando.
Para que eu possa montar o melhor roteiro turístico considerando avaliações e sugestões de outros usuários do aplicativo.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- A coleta de dados do usuário só poderá ocorrer com consentimento informado por ele.
- O aplicativo deve permitir que o usuário escolha o nível de precisão que deseja que sua geolocalização seja coletada.
- O aplicativo deve garantir que o usuário possa facilmente acessar e alterar suas preferências de privacidade a qualquer momento.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Location Granularity.</td></tr>
</table>

Figura 11. História de Usuário Utilizando o Padrão de Privacidade Location Granularity.

Decoupling [content] and Location Information Visibility

João é usuário de uma rede social e faz publicações diariamente. Recentemente, João notou que para cada *post* realizado, a rede social coleta, dentro de outros dados pessoais, a geolocalização do usuário. Porém, João não gostaria que sua geolocalização pudesse ser visualizada por todos os usuários da rede social, apenas por seus amigos e familiares quando for conveniente, garantindo assim sua privacidade.

Neste contexto, o padrão de privacidade Decoupling [content] and Location Information Visibility pode ser utilizado pois permite que os usuários decidam sobre a divulgação de informações de localização com relação ao contexto de um conteúdo específico. A Figura 12 descreve a história de usuário para o contexto supracitado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero decidir quais informações de geolocalização podem ser compartilhadas com determinadas pessoas.
Para que terceiros não autorizados obtenham acesso aos meus dados pessoais.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:
- Fotografia.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
</table>

Restrições: - O sistema deve armazenar, mediante consentimento informado pelo usuário, a sua geolocalização. - Permitir ao usuário desabilitar a função de coleta de geolocalização ao criar uma publicação. - Permitir ao usuário escolher quem poderá visualizar os dados de geolocalização coletados pelo sistema.
Recomendações de Padrões de Privacidade: - Decoupling [content] and Location Information Visibility.

Figura 12. História de Usuário Utilizando o Padrão de Privacidade Decoupling [content] and Location Information Visibility.

Active Broadcast of Presence

Fernanda utiliza um aplicativo de mensagens instantâneas para interagir com seus amigos e familiares. No entanto, ela gostaria de controlar como seu status é mostrado aos seus contatos para proteger a sua privacidade, além de auxiliá-la a se concentrar em outras tarefas sem ser interrompida constantemente.

Neste cenário, o padrão de privacidade Active Broadcast of Presence pode ser utilizado, pois possibilita que o aplicativo forneça ao usuário definir manualmente opções de presença, como online, disponível para conversar, ocupado, offline, invisível, entre outras. A Figura 13 exibe a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** controlar quando minha presença está ativa. **Para que** eu possa proteger minha privacidade e me concentrar em outras tarefas sem ser interrompido.		
Dados Pessoais: - Nome Completo. - Status. - Telefone.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Permitir ao usuário controlar como seu status será mostrado aos seus contatos. - Permitir ao usuário definir seu status como “offline” e “invisível” para não ser notificado ao receber mensagens. - Os contatos não poderão ser notificados da leitura das mensagens quando o status do receptor estiver como “offline” ou “invisível”.		
Recomendações de Padrões de Privacidade: - Active Broadcast of Presence.		

Figura 13. História de Usuário Utilizando o Padrão de Privacidade Active Broadcast of Presence.

Buddy List

Aline utiliza um aplicativo de mensagens instantâneas para interagir com seus contatos. Porém, preocupada com a privacidade de seus dados pessoais, Aline gostaria de limitar a visualização de suas informações pessoais, como nome completo, foto de perfil, telefone e status, apenas a contatos conhecidos e mantidos por ela em uma lista de pessoas confiáveis. Além disso, Aline gostaria que fosse possível adicionar novos contatos a lista e/ou remover contatos existentes para que estes não tenham mais acesso as suas informações pessoais.

Neste contexto, o padrão de privacidade Buddy List pode ser utilizado para garantir o controle de quais usuários serão permitidos em acessar informações pessoais do titular e quais informações pessoais serão compartilhadas com eles. A Figura 14 aborda a história de usuário para o exemplo mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero gerenciar uma lista de contatos que poderão visualizar meus dados pessoais.
Para que eu possa manter minhas informações pessoais privadas e seguras.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Status.
- Telefone.</td><td>Dados Pessoais Sensíveis:
- Fotografia.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Permitir ao usuário adicionar/remover outros usuários a sua lista de contatos.
- Restringir o acesso das informações pessoais do usuário aos contatos que estão adicionados à lista.
- Permitir ao usuário ocultar a lista de contatos para serem inacessíveis a outros usuários, mesmo aos contatos adicionados à lista.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Buddy List.</td></tr>
</table>

Figura 14. História de Usuário Utilizando o Padrão de Privacidade Buddy List.

Discouraging Blanket Strategies

Antônio é usuário de uma rede social e está preocupado que pessoas mal-intencionadas possam ter acesso de seus dados pessoais. Ele gostaria que a plataforma oferecesse aos usuários uma variedade de opções de privacidade, incluindo a possibilidade de limitar o acesso a determinados grupos de amigos ou conexões específicas. Além disso, Antônio considera relevante que a rede social

incentive seus usuários a revisar regularmente suas configurações de privacidade a fim de manter os dados pessoais seguros e protegidos.

Os anseios de Antônio podem ser atendidos por meio da implementação do padrão de privacidade Discouraging Blanket Strategies, que possibilita ao usuário definir um nível de privacidade para o conteúdo que será compartilhado. A história de usuário do exemplo é ilustrada na Figura 15.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero escolher o nível de privacidade para o conteúdo compartilhado.
Para que terceiros não autorizados não tenham acesso as informações compartilhadas.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Data de Nascimento.
- Informações pessoais que o usuário deseja compartilhar.</td><td>Dados Pessoais Sensíveis:
- Gênero</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Oferecer níveis de privacidade que poderão ser escolhidos para cada publicação realizada pelos usuários.
- Oferecer descrições claras e objetivas dos níveis de privacidade existentes. Exemplos visuais podem auxiliar na compreensão por parte dos usuários.
- Garantir que os usuários tenham controle sobre o compartilhamento de suas informações pessoais e possam escolher com quem compartilhá-las.
- Não permitir que os dados dos usuários sejam compartilhados com terceiros sem seu consentimento explícito.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Discouraging Blanket Strategies.</td></tr>
</table>

Figura 15. História de Usuário Utilizando o Padrão de Privacidade Discouraging Blanket Strategies.

As demais instâncias de padrões de privacidade encontram-se em sua totalidade no Apêndice G.

6.3 Exemplo de Utilização do PDSOP no Desenvolvimento Ágil

Para exemplificar a utilização do PDSOP, optou-se pelos processos ágeis de software Scrum e Kanban, visto que atualmente são os processos mais utilizados (MIRZA; DATTA, 2019; REDDY; KUMAR, 2020; VERSIONONE INC., 2022). Além disso, foram os processos de desenvolvimento de software mencionados nos estudos de caso descritos no Capítulo 5. A Subseção 6.3.1 e 6.3.2 apresentam o PDSOP integrado aos modelos Scrum e Kanban, respectivamente.

6.3.1 PDSOP Integrado ao Scrum

A Figura 16 apresenta o PDSOP integrado ao processo ágil Scrum. O processo foi dividido em duas atividades macro: Planejamento e Execução. Os elementos destacados em azul ciano são propostos neste trabalho, enquanto aqueles em preto pertencem ao Processo de Gerenciamento Ágil Scrum.

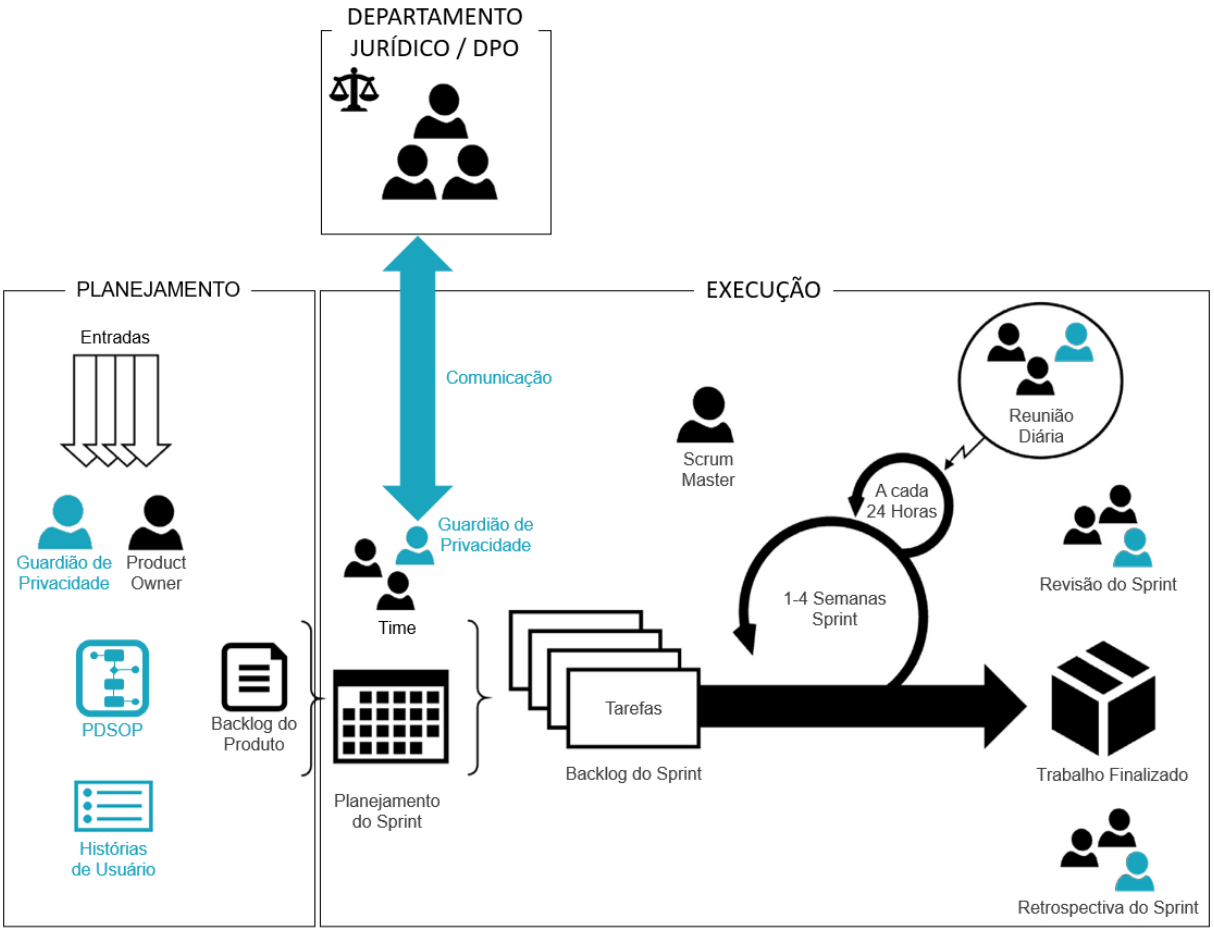

Figura 16. Representação do PDSOP Integrado ao Processo Ágil Scrum.

A primeira atividade do processo, Planejamento, tem como objetivo identificar os usuários do produto, suas expectativas, problemas e o valor agregado do produto que será desenvolvido para que atenda às expectativas do cliente e da equipe de desenvolvimento, identificados na imagem como “Entradas”.

Cada entrada, que podem ser Épicos e/ou Funcionalidades, também chamadas de *Feature*, necessita ser refinada a fim de expressar de maneira precisa os requisitos funcionais e não funcionais que farão parte daquela funcionalidade.

Conforme estabelecem os princípios do *Privacy by Design* (CAVOUKIAN, 2009a), os requisitos de privacidade de dados pessoais devem ser contemplados desde a primeira atividade de desenvolvimento de software. Para isto, o Guardião de Privacidade, juntamente com o Product Owner devem executar o PDSOP. Desta maneira, pode-se garantir que os requisitos de privacidade estejam em conformidade com as leis e regulamentos vigentes enquanto os interesses comerciais da organização são atendidos pelo Product Owner, conforme ilustra a Figura 16.

Com a execução do PDSOP os seguintes artefatos são gerados: (i) histórias de usuário, as quais, devem contar com os critérios de aceitação de privacidade, como dados pessoais, dados pessoais sensíveis, tempo de retenção, leis e regulamentos, restrições, e recomendação de padrões de privacidade, conforme proposto na Figura 10; e (ii) backlog do produto, que contém todas as histórias de usuário que serão posteriormente implementadas.

O backlog do produto é definido pelo processo Scrum e visa garantir que todos os aspectos do produto sejam considerados e planejados de acordo com o tempo e recurso de cada time de desenvolvimento. Por este motivo, as histórias de usuário podem ser continuamente priorizadas pelo Product Owner à medida que novos requisitos são identificados.

Na segunda atividade do processo, denominada Execução, ocorre o desenvolvimento do produto de software. Caso o time de desenvolvimento esteja na primeira iteração do modelo de processo, o objetivo deve ser de preparação do ambiente. Neste caso, os membros da equipe estabelecem o escopo, metas e tarefas para o desenvolvimento, além da infraestrutura técnica necessária para o sucesso do projeto. Esta etapa é chamada de Sprint 0 (zero).

Nas iterações seguintes, são realizadas as reuniões de planejamento do Sprint, nas quais, o Scrum Master, Product Owner e o time de desenvolvimento, incluindo o Guardião de Privacidade, selecionam os itens de maior prioridade presentes no Backlog do Produto. Estes itens de maior prioridade serão desenvolvidos e entregues no Sprint atual, garantindo *releases* de maneira contínua aos clientes.

Durante as iterações de desenvolvimento, denominados Sprints, a equipe trabalha no desenvolvimento dos itens selecionados. Cada Sprint pode durar entre uma e quatro semanas, sendo de responsabilidade dos membros do time de desenvolvimento definir a data da próxima entrega. Nesta atividade, os integrantes da equipe trabalham em conjunto a fim de alcançar os objetivos do Sprint. Além disso, o

Guardião de Privacidade deve monitorar e garantir que as medidas de privacidade de dados estejam integradas no desenvolvimento do software. Caso surjam dúvidas, ele deve ser o canal de comunicação entre o time de desenvolvimento e o departamento jurídico e/ou o DPO da organização.

Após o início do Sprint, todos os dias devem ser realizadas as reuniões diárias, nas quais os membros do time devem responder três perguntas:

- o que você fez no dia anterior?
- o que você está planejando fazer no dia de hoje?
- há algum problema que lhe impeça de realizar seu objetivo?

Ao final do Sprint, o time realiza a Revisão do Sprint. Nesta reunião é demonstrado o trabalho concluído ao Product Owner e outros *stakeholders*. Há discussões do que foi alcançado, o que precisa ser melhorado e o que está sendo preparado para o próximo Sprint. Além da Revisão do Sprint, há também Retrospectiva do Sprint, em que o time se reúne para refletir sobre o Sprint anterior. Esta reunião visa identificar quais foram os pontos positivos e negativos para que os integrantes da equipe proponham melhorias aos procedimentos que julgarem necessários, inclusive o Guardião de Privacidade, que pode desenvolver e revisar políticas e procedimentos de privacidade de dados para o próprio time ou para a organização como um todo.

6.3.2 PDSOP Integrado ao Kanban

Conforme mencionado na Seção 2.1.2, o objetivo do quadro Kanban é melhorar o fluxo de trabalho de equipes que estão oferecendo um serviço ou produto aos seus clientes (STEYAERT, 2017). Para isto, Anderson (2010) define três possíveis estados para as atividades a serem implementadas: planejada, em andamento, e concluída. No quadro Kanban os estados são representados por colunas e as atividades por cartões que iniciam na coluna “planejada” e avançam para as colunas subsequentes até atingirem o fim do fluxo, coluna “concluída”. No entanto, o quadro Kanban tem como principal vantagem a adaptabilidade, o que permite que equipes ajustem o fluxo de trabalho às suas necessidades e circunstâncias, como por exemplo, incluir ou remover colunas, definir e modificar o número de trabalho em progresso, alterar a prioridade de cartões, entre outros.

Segundo Steyaert (2017), para uma atividade ser fixada à coluna “planejada” ela deve estar apta a ser implementadas pelo time de desenvolvimento e, consequentemente, não pode estar escrita de maneira a gerar dúvidas. Por este motivo, o autor defende que sejam realizadas adaptações ao quadro Kanban para que etapas de amadurecimento e validação sejam contempladas preliminarmente ao primeiro estado especificado por Anderson (2010).

Na prática, verificou-se que o argumento de Steyaert (2017) foi implementado nas organizações entrevistadas (Apêndice D). As organizações que utilizam o quadro Kanban em seus projetos de desenvolvimento de software realizaram adaptações para atenderem melhor suas demandas, conforme mencionado pelos colaboradores das Organizações C e E.

Ao considerar a revisão da literatura e os estudos de casos conduzidos, optou-se por ilustrar o quadro Kanban contendo um fluxo de atividades detalhado, aproximando-se da dinâmica identificada nas organizações entrevistadas. Essa escolha visa proporcionar uma representação fiel e específica das práticas adotadas, permitindo uma análise precisa e comparativa em relação aos contextos observados nas organizações estudadas.

Sendo assim, organizou-se o fluxo geral de desenvolvimento em atividades de “Escrita de Histórias de Usuário” (Figura 17) e “Desenvolvimento” (Figura 18). A Figura 17 ilustra as atividades responsáveis pela descoberta, exploração/refinamento e escrita de histórias de usuário. Os itens apresentados em azul ciano são propostos neste estudo, enquanto os destacados em preto estão associados ao método Kanban.

A “Descoberta” abrange as atividades de pesquisa, descoberta de requisitos e design do produto. Essa etapa é importante para ajudar as equipes a compreenderem o que precisam construir e os motivos. Esta atividade pode incluir análise de dados, estudo de mercado e prototipagem de soluções. Ao conduzir essas tarefas, as equipes podem identificar os requisitos do produto, avaliar as necessidades do cliente e garantir que a solução tenha um design coerente e funcional.

Na “Exploração/Refinamento”, os times de desenvolvimento buscam especificar os detalhes dos requisitos do produto e explorar diferentes soluções para atender as novas demandas. Para isto, podem criar protótipos detalhados, realizar entrevistas com clientes e coletar *feedback* dos usuários para reduzir o risco de desenvolver produtos que não atendam às necessidades do público-alvo. Ao optar

por prosseguir com a implementação dos novos requisitos, pode-se aplicar o PDSOP (Figura 9) para a escrita de histórias de usuário.

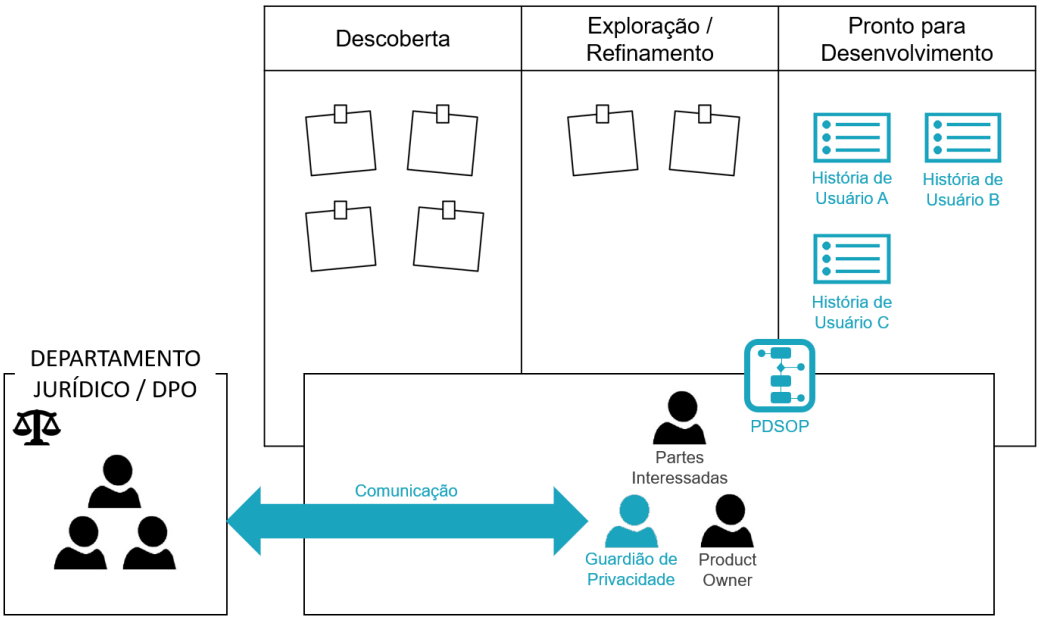

Figura 17. Representação do PDSOP Implementado nas atividades de Escrita de Histórias de Usuário.

Para garantir conformidade legal e os devidos cuidados com a privacidade de dados pessoais, os profissionais responsáveis pela execução do PDSOP são o Product Owner e Guardião de Privacidade. Após a execução do PDSOP, histórias de usuário contendo os critérios de aceitação de privacidade (Figura 10) podem ser adicionadas à coluna subsequente, “Pronto para Desenvolvimento”. Nesta coluna encontram-se uma lista priorizada de histórias de usuários que precisam ser implementadas para que o produto seja concluído, sendo de responsabilidade do Product Owner priorizá-las considerando o valor de negócio para o cliente e as metas organizacionais. Se em algum momento destas atividades surgirem dúvidas legais, é de responsabilidade do Guardião de Privacidade consultar o departamento jurídico e/ou o DPO a fim de saná-las.

Uma vez que haja histórias de usuários prontas para desenvolvimento, o time pode selecionar algumas destas histórias para serem movidas para “Em Desenvolvimento”. A Figura 18 apresenta as atividades de desenvolvimento, testes, homologação e produção das histórias de usuário. Para este exemplo, todas as histórias de usuário encontram-se na cor azul ciano, indicando que são artefatos gerados a partir da execução do PDSOP, seguindo o padrão apresentado na Figura 10.

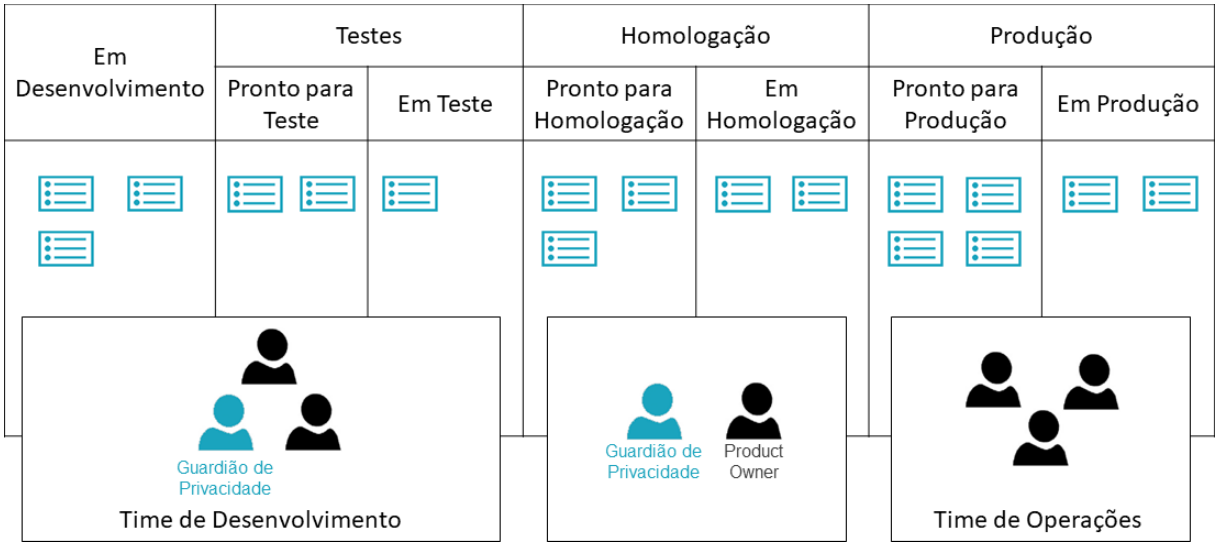

Figura 18. Representação do PDSOP Implementado nas atividades de Desenvolvimento.

A primeira coluna, denominada “Em Desenvolvimento”, refere-se às histórias de usuário que estão sendo implementadas pelo time de desenvolvimento. Uma vez finalizada esta atividade, a história é movida para a próxima coluna, “Pronto para Teste”. Esta coluna identifica que as histórias foram desenvolvidas, porém ainda necessitam de testes para serem homologadas.

Em um momento oportuno, a equipe, ou um membro desta, pode deslocar a história para a coluna “Em Teste” e iniciar os testes referentes àquela história. Tanto a atividade de desenvolvimento quanto de teste é de responsabilidade do time de desenvolvimento realizá-las, verificando se as histórias contêm os requisitos anteriormente elicitados.

Após realizar todos os testes, a história de usuário pode ser movida para a coluna “Pronto para Homologação”. A partir deste estado, é de responsabilidade do Product Owner realizar os testes finais no produto em ambiente semelhante ao de produção. Esta verificação visa garantir que o software atenda às especificações do usuário, seja seguro, confiável e esteja apto para ser implantado, não causando problemas ou conflitos com outras funcionalidades do software.

O Guardião de Privacidade tem a responsabilidade de verificar se os requisitos de privacidade de dados pessoais foram devidamente implementados e se o produto está em conformidade legal com as leis e regulamentos vigentes. Se o Guardião de Privacidade for um profissional específico a este fim ou se o profissional com estas atribuições for o Analista de Qualidade, a verificação pode ocorrer no ambiente de desenvolvimento, coluna “Em Teste”. Entretanto, se o colaborador incumbido da

averiguação dos requisitos de privacidade for um Arquiteto de Soluções ou Líder Técnico, poderá desempenhar suas funções junto ao Product Owner, na etapa de homologação, coluna “Em Homologação”.

Após a história de usuário ser homologada, poderá ser movida para a coluna “Pronto para Produção”, na qual, no momento adequado, a nova funcionalidade é implantada no ambiente real de produção para que os usuários possam interagir e usar. Nesta mesma atividade, o time de operações deve trabalhar para garantir que tudo esteja funcionando conforme o esperado. Isso pode incluir a monitoração de *logs*, rastreamento de erros e verificação de desempenho.

6.4 Repositório de Informações

O repositório foi concebido para consolidar as informações necessárias para uso do PDSOP, em um único ambiente. Ele busca otimizar o tempo gasto pelos desenvolvedores e demais profissionais envolvidos nos projetos de desenvolvimento de software, permitindo um acesso de maneira rápida e eficiente às informações necessárias.

A página inicial do repositório é apresentada na Figura 19, na qual é exibido o PDSOP, além das explicações das atividades e artefatos que compõem o processo. Cada atividade é detalhada em tarefas, ilustrando o que deve ser realizado pelo Guardião de Privacidade e qual é o resultado esperado como saída da atividade, conforme descrito na Seção 6.1.

No topo da página encontram-se um menu que possibilita ao usuário navegar no repositório. As opções são: Processo, História de Usuário, Guardião de Privacidade, Exemplo de Integração e Padrões de Privacidade.

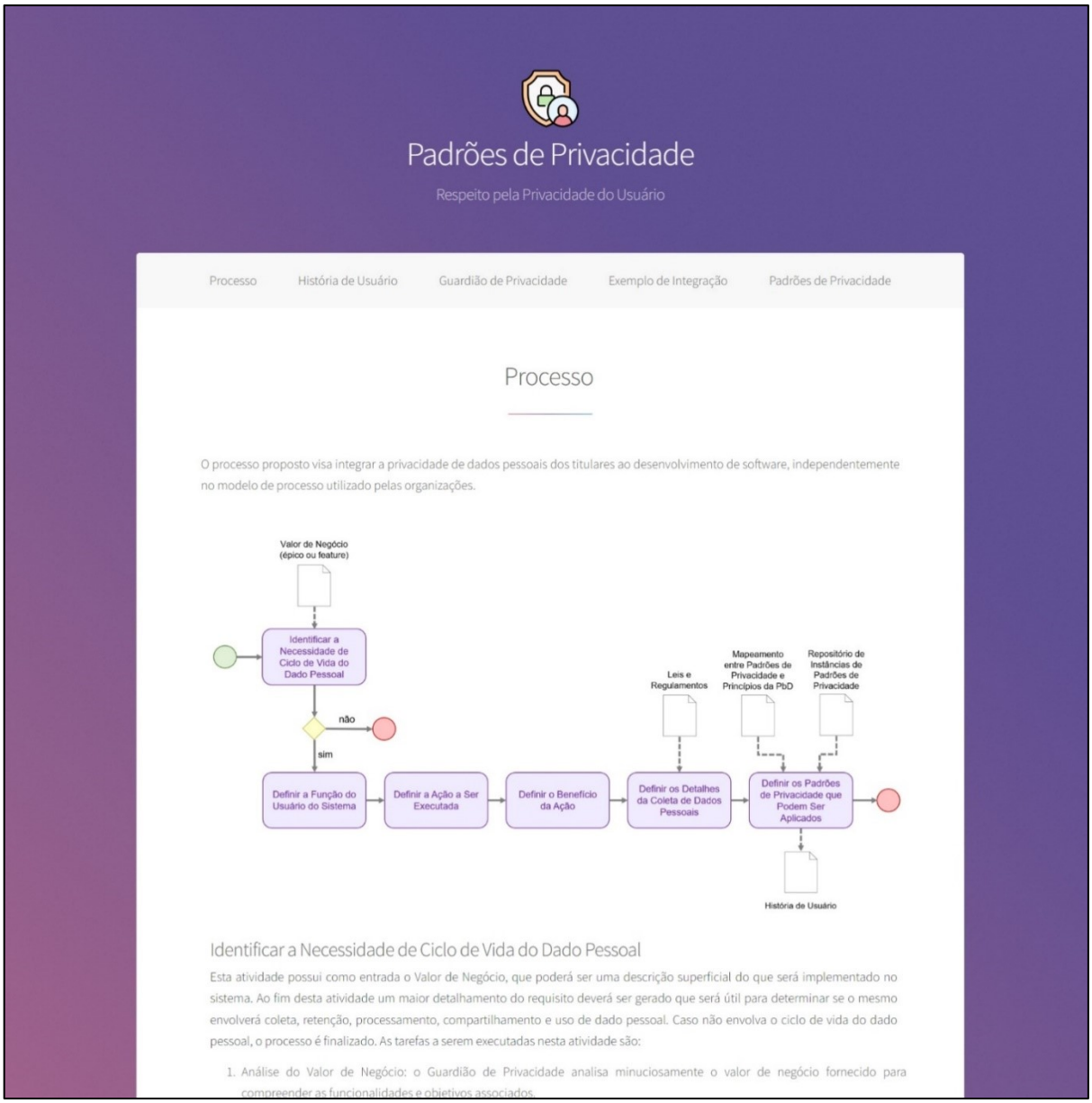

Figura 19. Página Processo.

Ao clicar na opção História de Usuário, o usuário é redirecionado à página que apresenta o artefato gerado ao fim do PDSOP, uma História de Usuário contemplando critérios de privacidade de dados pessoais, por exemplo, dados pessoais, dados pessoais sensíveis, tempo de retenção, leis e regulamentos citados, restrições e recomendações de Padrões de Privacidade, conforme apresentado na Subseção 6.2.1. A Figura 20 apresenta a página de História de Usuário.

Figura 20. Página História de Usuário.

A opção Guardião de Privacidade redireciona o usuário à página do papel do Guardião de Privacidade. Nesta página são destacadas as informações relativas ao papel, como perfil esperado, atividades do processo pelas quais é responsável, atuação na organização, tanto no time de desenvolvimento quanto no âmbito organizacional, treinamentos recomendados e vantagens do papel na composição dos times de desenvolvimento, conforme definido na Seção 6.1. A Figura 21 apresenta a página do Guardião de Privacidade.

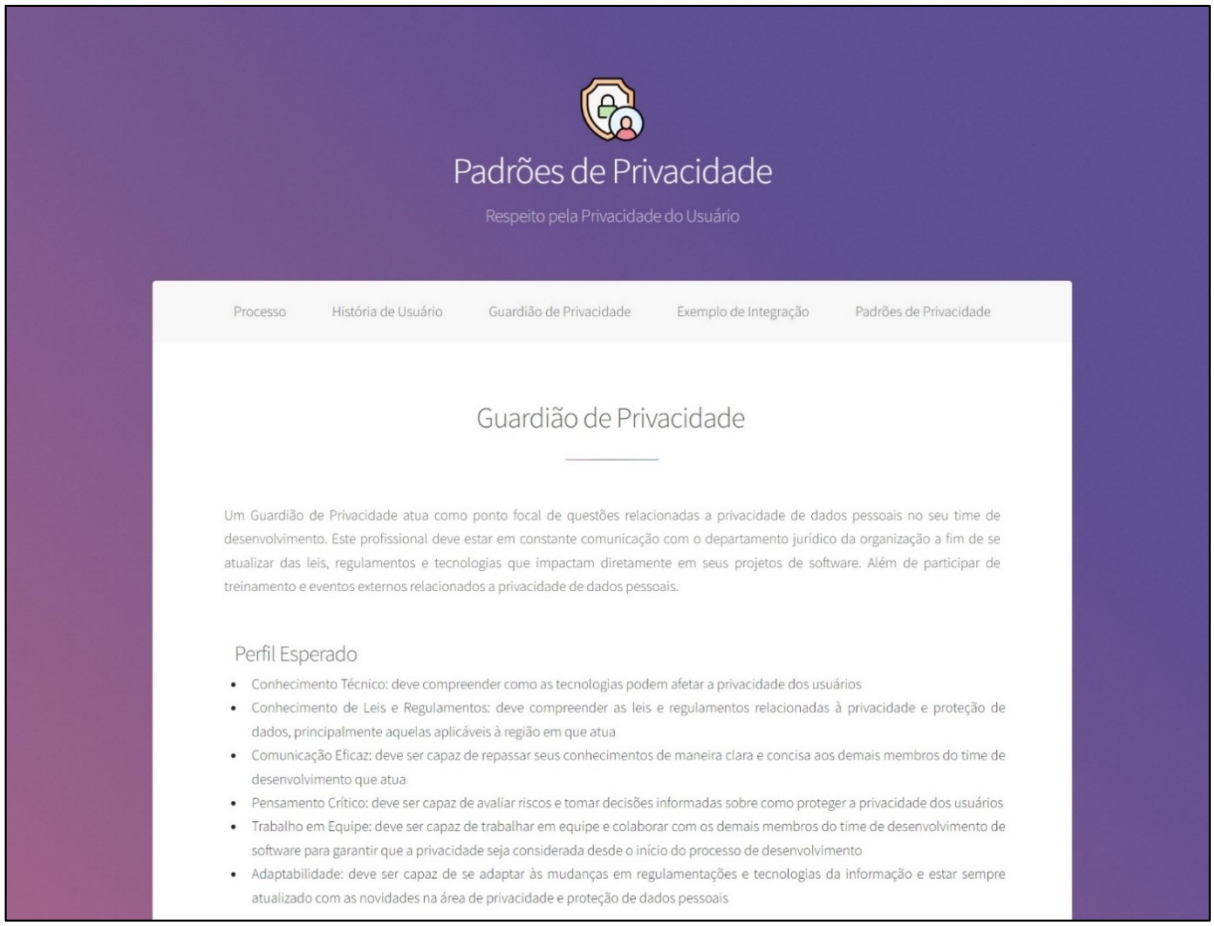

Figura 21. Página Guardião de Privacidade.

A Figura 22 apresenta a página de exemplo de integração do PDSOP. Nesta página encontram-se informações textuais e figuras de exemplos de como o PDSOP pode ser utilizado de modo integrado aos processos Scrum e/ou Kanban, apontando as atividades dos processos que devem ser adaptadas e como o Guardião de Privacidade atua em cada processo, conforme apresentado na Seção 6.3.

Figura 22. Página Exemplo de Integração.

Por fim, a opção de Padrões de Privacidade exibe a coleção dos padrões de privacidade catalogadas pela Universidade da Califórnia (UC BERKELEY SCHOOL OF INFORMATION, 2024) e abordados neste trabalho. Nesta página é apresentado apenas os nomes dos padrões. Caso o usuário deseje obter detalhes de um padrão específico, ele deve pressionar o link “Visualizar”, à direita do padrão desejado. A Figura 23 apresenta a página Padrões de Privacidade.

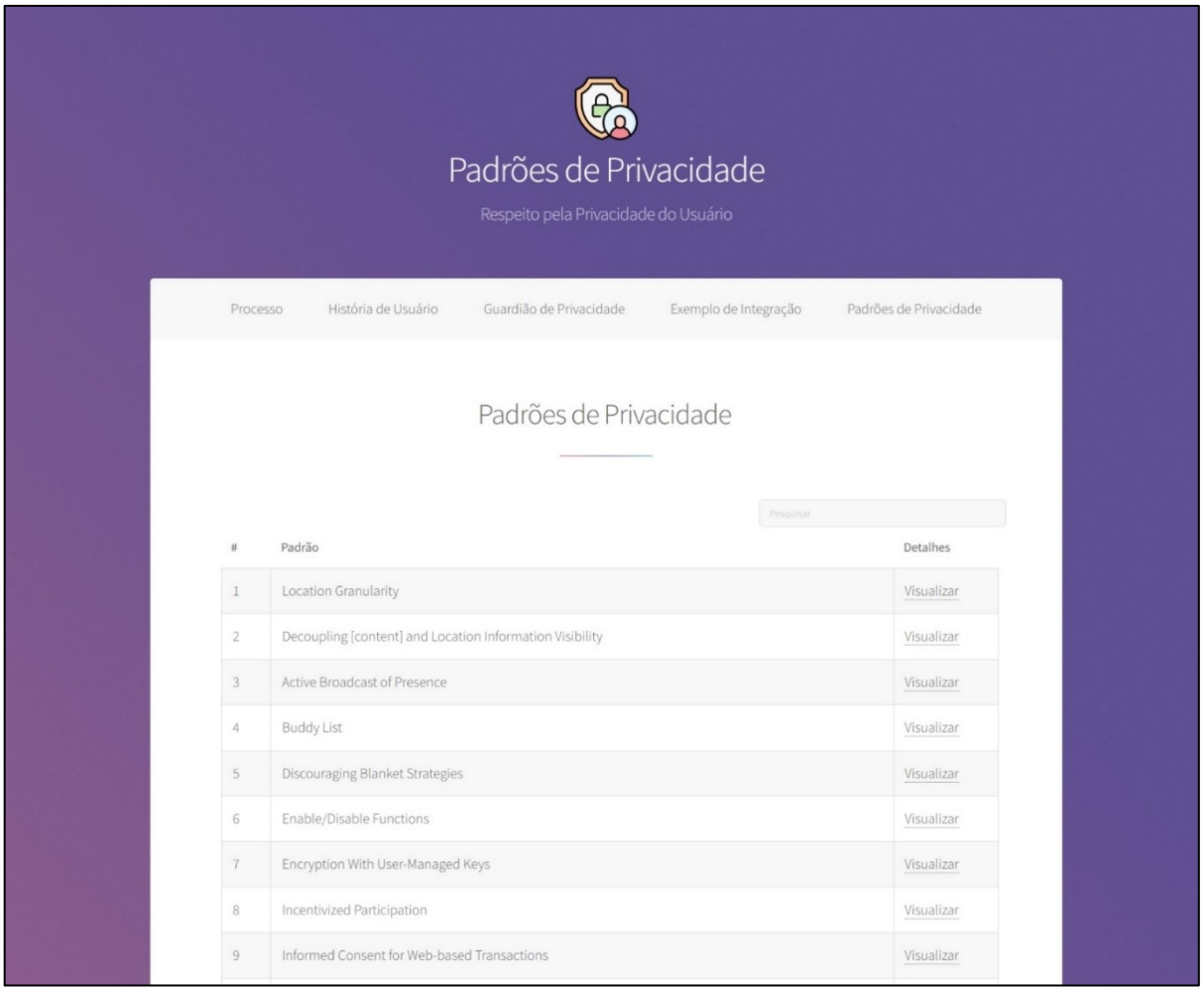

Figura 23. Página Padrões de Privacidade.

Além disso, a funcionalidade de filtragem oferecida pela ferramenta desempenha um papel fundamental na personalização da experiência do usuário. Um campo dedicado foi incorporado à interface, localizado acima da lista de padrões de privacidade. Ao digitar palavras-chave ou termos no campo de filtro, o software realiza uma busca, trazendo à página apenas os padrões de privacidade que correspondem diretamente aos critérios fornecidos pelo usuário. Essa abordagem visa simplificar ainda mais o acesso à informação, garantindo que os desenvolvedores encontrem de maneira rápida e precisa o conteúdo desejado, otimizando assim o fluxo de trabalho diário.

A Figura 24 ilustra a busca pelo termo “localização”. Neste caso, são apresentados apenas três padrões de privacidade: *Location Granularity*, *Decoupling [Content] and Location Information Visibility* e *Active Broadcast of Presence*.

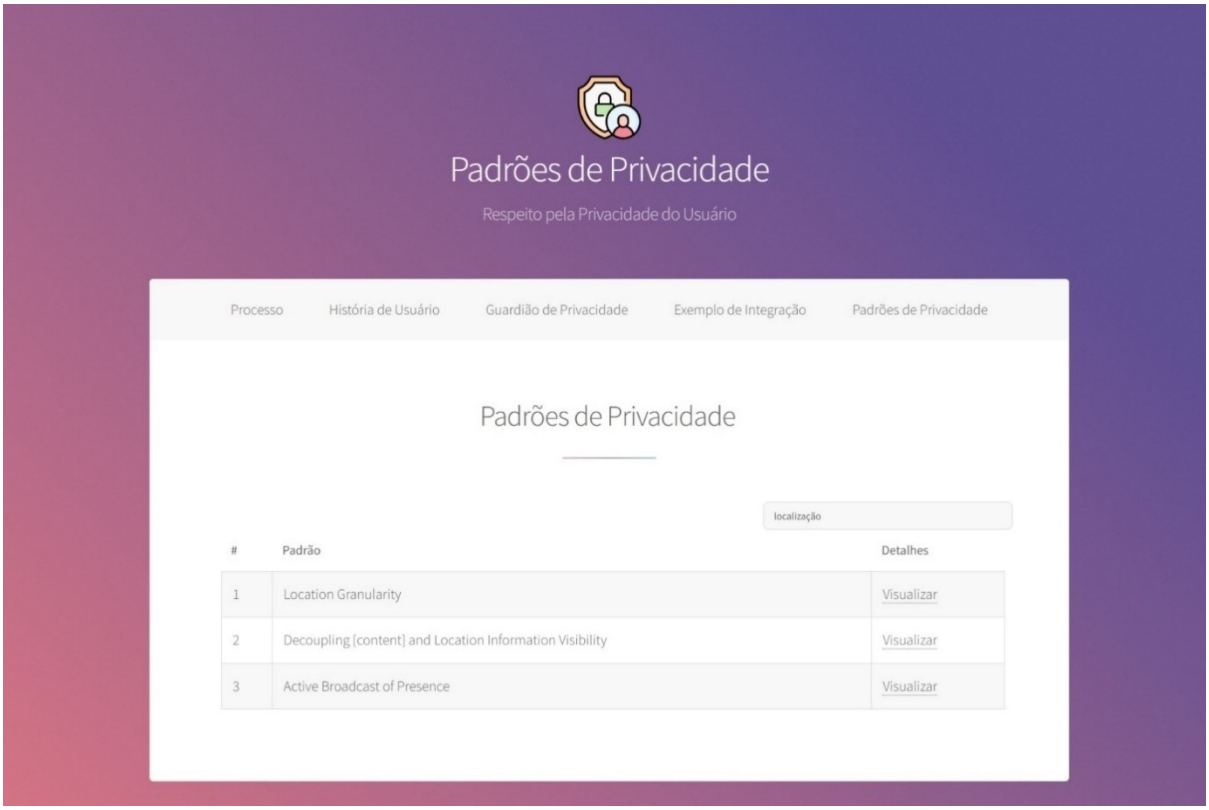

Figura 24. Uso do Filtro na Página Padrões de Privacidade.

Ao pressionar a opção “Visualizar” de um padrão de privacidade, uma nova página é apresentada contendo as informações do padrão, como:

- Nome
- *Labels*;
- Contexto;
- Problema;
- Solução;
- Princípios do *Privacy by Design*; e
- Estratégias de Hoepman.

A Figura 25 destaca os detalhes do Padrão de Privacidade *Location Granularity*.

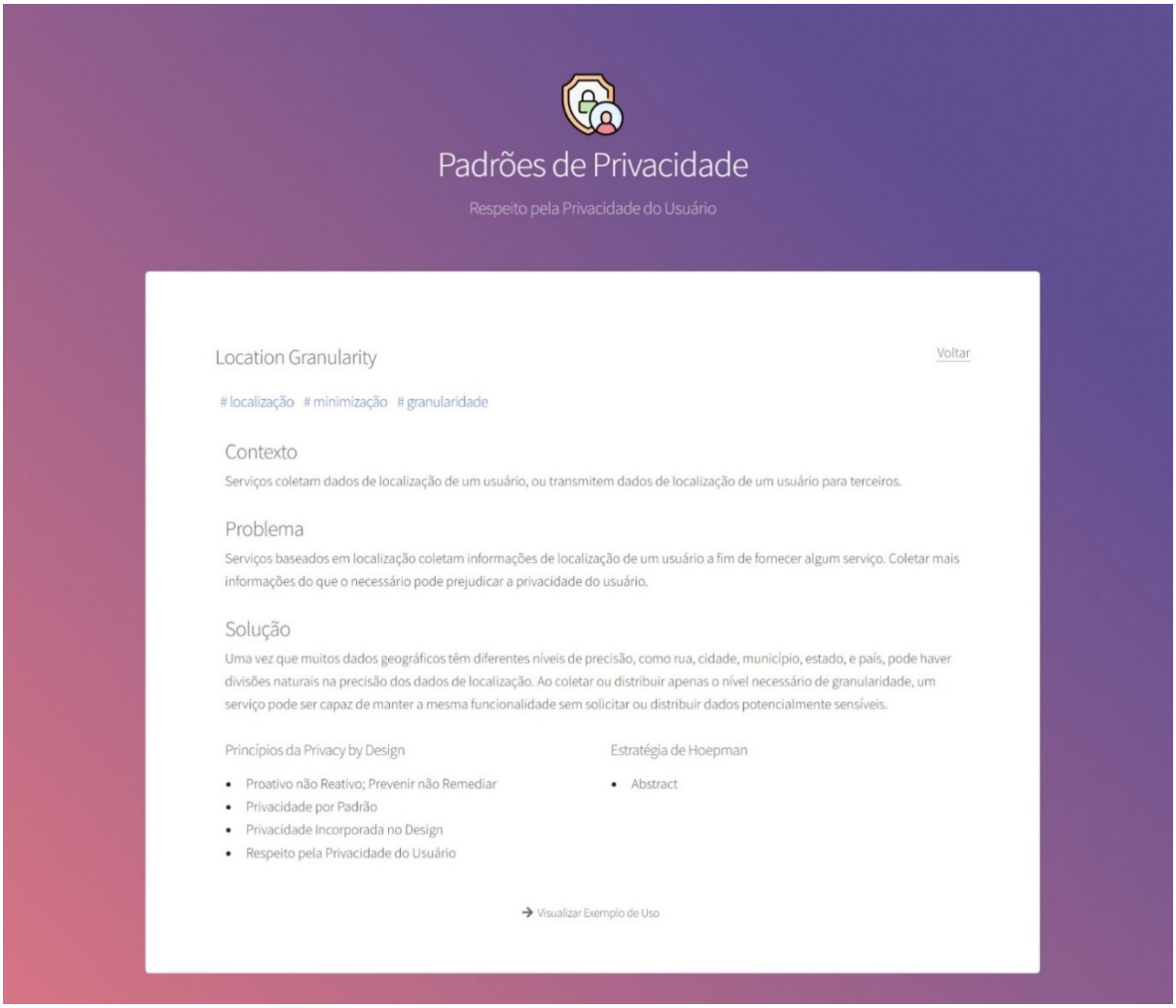

Figura 25. Detalhes do Padrão de Privacidade Location Granularity.

Para o padrão *Location Granularity* foram definidos os *labels*: localização, minimização e granularidade. Estes termos auxiliam na busca dos padrões, que filtra e mostra os resultados com uma melhor acurácia. Entretanto, todas as informações dos padrões são consideradas na busca, não somente os *labels*.

As informações referentes aos princípios do PbD que o padrão *Location Granularity* contempla são obtidas a partir do artefato “Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design*”, apresentados na Subseção 6.2.2. Neste exemplo, o padrão *Location Granularity* está associado aos princípios (i) Proativo não Reativo; Prevenir não Remediar; (ii) Privacidade por Padrão; (iii) Privacidade Incorporada no Design; e (vii) Respeito pela Privacidade do Usuário, conforme Quadro 9, página 98.

Para cada padrão de privacidade apresentado, há um exemplo de aplicação. Para acessá-lo, é necessário que o desenvolvedor pressione o link “Visualizar

Exemplo de Uso”, disponível no fim da página. A Figura 26 detalha o exemplo de uso do padrão de privacidade Location Granularity. Estas informações são obtidas a partir do artefato “Repositório de Instâncias de Padrões de Privacidade” (Subseção 6.2.3), no qual são apresentados contextos para os quais os padrões de privacidade podem ser aplicados. Ao final, uma história de usuário é escrita contendo os detalhes de privacidade, conforme o artefato “História de Usuário”, apresentado na Figura 10, Subseção 6.2.1.

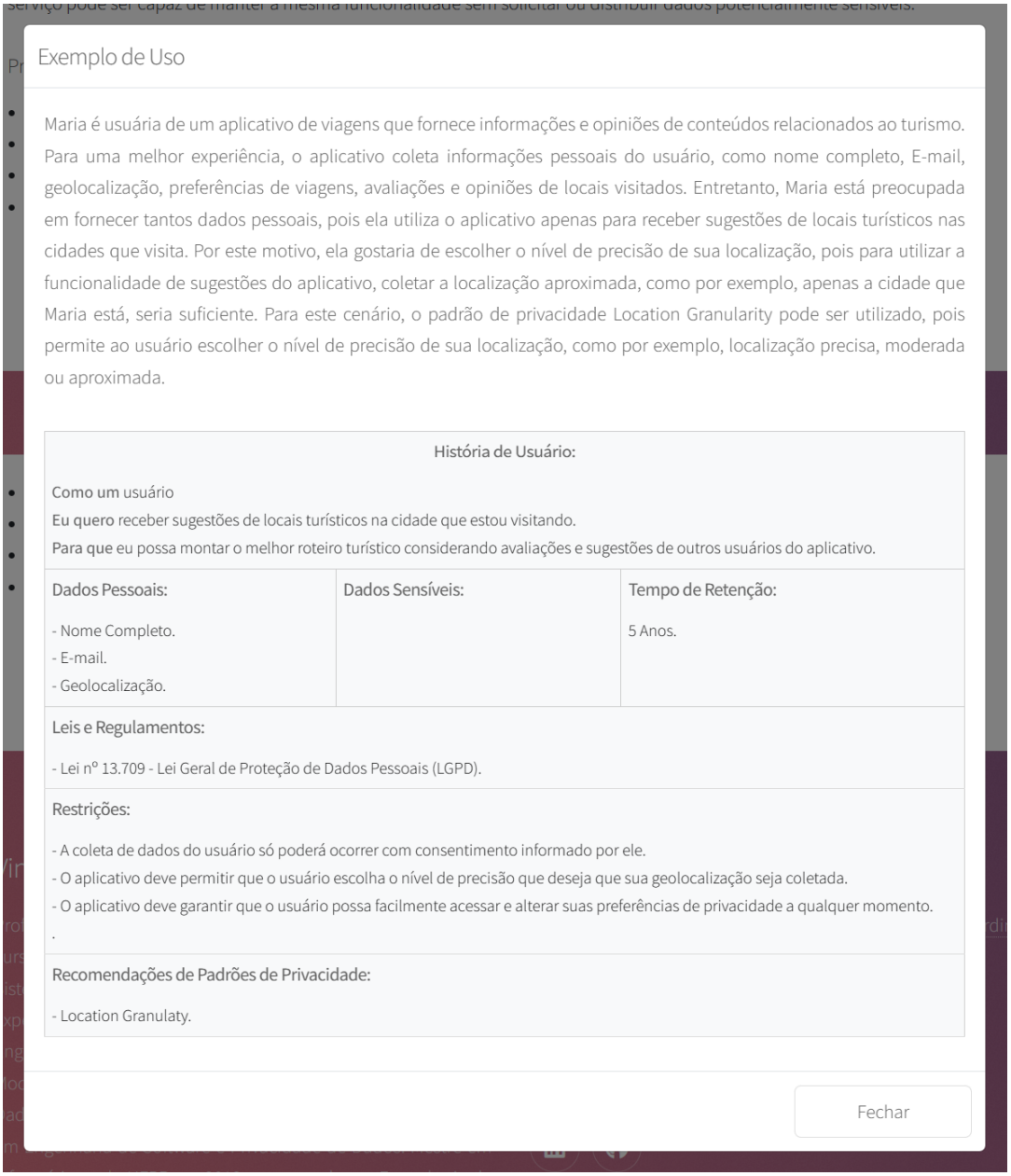

Figura 26. Exemplo de Uso do Padrão de Privacidade.

6.5 Considerações sobre o Capítulo

Este capítulo apresentou o processo e os artefatos propostos: História de Usuário; Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design*; e Repositório de Instâncias de Padrões de Privacidade, assim como o Guardião de Privacidade. Além disso, foram ilustrados exemplos da integração do PDSOP aos processos de desenvolvimento de software já consolidados nas organizações, como Scrum e Kanban. Para estas integrações, foram abordadas quais adaptações devem ser realizadas a fim de possibilitar ao time de desenvolvimento obter o máximo de proveito do PDSOP sem que seja necessário alterar completamente o processo já em andamento na organização.

Por fim, foi apresentado um repositório que centraliza as informações para facilitar aos desenvolvedores a obtenção dos detalhes, tanto do processo quanto do papel e artefatos propostos.

O Capítulo 7 apresenta a avaliação do processo realizada por meio de especialistas em privacidade de dados pessoais e desenvolvimento de software.

CAPÍTULO 7 - AVALIAÇÃO DO PROCESSO

Este capítulo apresenta os resultados obtidos a partir da avaliação do processo com a participação de especialistas. A Seção 7.1 apresenta os dados de perfil dos especialistas que participaram da avaliação. A Seção 7.2 aborda os resultados das avaliações realizadas junto aos especialistas. A Seção 7.3 discute os resultados obtidos. A Seção 7.4 descreve as ameaças a validade da avaliação. Por fim, a Seção 7.5 destaca as considerações sobre o capítulo.

7.1 Perfil dos Especialistas

A Tabela 1 apresenta os dados de cada especialista que participou desta avaliação, conforme a ordem em que os dados foram enviados por meio do formulário eletrônico (Apêndice A.4).

Tabela 1. Dados do Perfil dos Especialistas da Avaliação.

Id	Nível de Formação	Cargo/Função	Experiência na área	Experiência com Desenvolv. de Software	Experiência com Privac. de Dados Pessoais
Avaliação com Especialistas (N = 11)					
01	Mestre	Gerente de Tecnologia e Transformação	10 anos	Avançada	Avançada
02	Mestre	Engenheiro de Software	10 anos	Moderada	Moderada
03	Doutor	Tech Lead	23 anos	Avançada	Moderada
04	Especialista	Engenheiro de Software	9 anos	Moderada	Avançada
05	Mestre	Coordenador Regional de Dados & Analytics	15 anos	Avançada	Avançada
06	Especialista	Coordenador de Arquitetura e Segurança da Informação	12 anos	Avançada	Avançada
07	Especialista	Líder de Teste	17 anos	Avançada	Moderada
08	Mestre	Especialista em Arquitetura de Soluções	20 anos	Avançada	Avançada

09	Especialista	Coordenador de TI	15 anos	Moderada	Moderada
10	Especialista	Product Owner	13 anos	Moderada	Moderada
11	Especialista	Head de Segurança da Informação e DPO	15 anos	Moderada	Avançada
Moda					
	Especialista		14 anos (em média)	Avançada	Avançada

Para a realização da avaliação, cada especialista preencheu o Termo de Consentimento Livre e Esclarecido (Apêndice A.3) e o Questionário de Caracterização de Perfil (Apêndice A.4). Para considerar uma avaliação válida, o especialista deveria ter experiência Moderada ou Avançada (conforme critérios estabelecidos no Questionário de Caracterização de Perfil – Apêndice A.4) nas questões de desenvolvimento de software e privacidade de dados pessoais, não sendo estabelecido um determinado cargo/função específico. Sendo assim, a Tabela 1 apresenta apenas os dados dos especialistas que satisfizeram os requisitos mínimos necessários.

De acordo com as respostas fornecidas, nota-se que seis avaliadores possuem nível de formação especialista, quatro mestres e um doutor. Atualmente, os avaliadores são colaboradores de diversas organizações de desenvolvimento de software, desempenhando diferentes cargos e funções, além de possuírem diferentes anos de experiência na área. A média de experiência é de 14 anos.

No que diz respeito ao conhecimento dos avaliadores em desenvolvimento de software e privacidade de dados pessoais, seis mencionaram que possuem experiência avançada e cinco moderada, em cada um dos assuntos. Sendo assim, a moda[38] referente a experiência é avançada, tanto para o desenvolvimento de software quanto para privacidade de dados pessoais.

7.2 Resultados

Todos os 11 (onze) especialistas responderam ao questionário de avaliação (Apêndice H), que possui 9 (nove) questões de múltipla escolha que utilizam a escala

[38] Moda: a moda amostral de um conjunto de dados trata do valor que ocorre com maior frequência ou o valor mais comum em um conjunto de dados (GUJARATI; PORTER, 2010).

de *Likert* com 5 (cinco) itens: Discordo Totalmente; Discordo Parcialmente; Não Discordo e Não Concordo; Concordo Parcialmente; e Concordo Totalmente.

Para cada uma das 9 (nove) questões respondidas pelos avaliadores, eles foram incentivados a relatar o motivo da nota atribuída, apontar pontos positivos, limitações e melhorias, de acordo com a facilidade de uso, utilidade e intenção de uso futuro, conforme fundamentado no *Technology Acceptance Model (TAM 3)* (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008).

Por meio da análise das respostas de múltipla escolha utilizando a Codificação Magnitude (SALDAÑA, 2013), foi possível obter informações sobre o grau de concordância entre os especialistas em relação ao uso geral dos artefatos, papel e processo propostos.

A Tabela 2 apresenta as notas atribuídas pelos especialistas em cada umas das questões de múltipla escolha.

Tabela 2. Respostas dos Especialistas Considerando Questões Baseadas no TAM3.

Especialista Id #:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
Facilidade de Uso - Ease of Use (E)											
E1. O processo proposto é compreensível.	5	5	5	5	5	5	5	4	5	5	5
E2. Os artefatos (i) Mapeamento dos Padrões de Privacidade e Princípios do *Privacy by Design* e (ii) Repositório de Histórias de Usuário são compreensíveis.	4	5	5	4	5	5	5	5	5	5	4
E3. As responsabilidades do Guardião de Privacidade são compreensíveis.	5	4	4	5	4	5	4	3	4	5	5
E4. Acho fácil incluir o processo proposto no processo de desenvolvimento que é utilizado atualmente na organização.	4	3	4	4	4	3	4	5	5	2	2
Utilidade - Usefulness (U)											
U1. A utilização do processo fará com que os requisitos de privacidade de dados pessoais sejam considerados desde o início do processo de desenvolvimento de software.	5	4	5	4	5	5	5	4	5	5	5
U2. A utilização do processo evitará o retrabalho da aplicação de requisitos de privacidade de dados pessoais do time de desenvolvimento de software.	4	5	5	4	5	5	5	5	5	5	5
U3. Eu considero o processo útil para implementar requisitos de privacidade de dados pessoais.	4	5	5	5	5	5	5	5	5	5	5
U4. Eu recomendaria o processo de privacidade para engenheiros de software.	5	5	5	4	4	5	5	4	5	5	5

Intenção de Uso - Intention of Use (I)											
I1. Eu utilizaria o processo proposto no desenvolvimento de software da organização.	4	5	4	4	3	5	5	5	5	5	5

Legenda	**Escala TAM (*Likert*)**
Discordo Totalmente	1
Discordo Parcialmente	2
Não Discordo e Não Concordo	3
Concordo Parcialmente	4
Concordo Totalmente	5

Os resultados da análise das respostas dos especialistas foram positivos, embora sua capacidade de generalizar o uso dos artefatos seja limitada. O Coeficiente de Correlação Intraclasse (ICC) foi calculado para avaliar a confiabilidade e reprodutividade interobservadores para comparar a consistência e a concordância entre as notas atribuídas pelos 11 (onze) especialistas. A Tabela 3 apresenta o resultado do ICC, bem como o intervalo de confiança e o Teste F.

Tabela 3. Coeficiente de Correlação Intraclasse para as Respostas dos Especialistas.

Correlação Intraclasse	Intervalo de Confiança de 95%		Teste F	
	Limite Inferior	Limite Superior	Valor	Significância
0,810	0,554	0,950	5,175	0,000

Segundo Koo e Li (2016), um ICC pode ser classificado como:

- Confiabilidade Pobre: ICC < 0,50;
- Confiabilidade Moderada: ICC >= 0,50 e < 0,75;
- Confiabilidade Boa: ICC >= 0,75 e <= 0,90;
- Confiabilidade Excelente: ICC > 0,90.

Ao considerar um intervalo de confiança de 95%, obteve-se um limite inferior de 0,554 e superior de 0,950, o que indica 95% de confiança de que o valor do ICC está entre ambos os valores. O Teste F, que tem como intuito comparar as médias de dois ou mais grupos e determinar se existem diferenças significativas entre elas, apresentou o valor de 5,175, com significância de 0,000, o que sugere que a variação entre os especialistas é estatisticamente significativa. Por fim, o valor do ICC foi de 0,810 (81%), o que indica, segundo Koo e Li (2016), uma **boa confiabilidade** entre as notas atribuídas pelos 11 (onze) especialistas.

A análise das questões de múltipla escolha (quantitativas) foi complementada pela análise das questões abertas (qualitativas), as quais foram interpretadas após a aplicação do processo de Codificação Provisória (SALDAÑA, 2013). Os códigos e subcódigos resultantes desse processo são:

- Facilidade de Uso;
- Utilidade;
- Intenção de Uso Futuro;
- Aspectos Positivos – Artefatos;
- Aspectos Positivos – Guardião de Privacidade;
- Aspectos Positivos – Processo;
- Limitações – Artefatos;
- Limitações – Guardião de Privacidade;
- Limitações – Processo;
- Recomendações de Uso; e
- Sugestões de Melhorias.

No que diz respeito à Facilidade de Uso, esta avaliação aborda a percepção e o esforço dos especialistas em relação ao processo, papel e artefatos propostos, com base nos princípios do TAM 3 (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008). A Figura 27 apresenta uma rede (criada no ATLAS.ti, versão 9) contendo trechos de texto que representam a facilidade de uso do processo, que fazem parte deste processo de codificação. Alguns especialistas se limitaram a dizer que o processo é fácil de se utilizar, não detalhando o motivo da nota atribuída. Para estes casos, o trecho da avaliação não se encontra na rede.

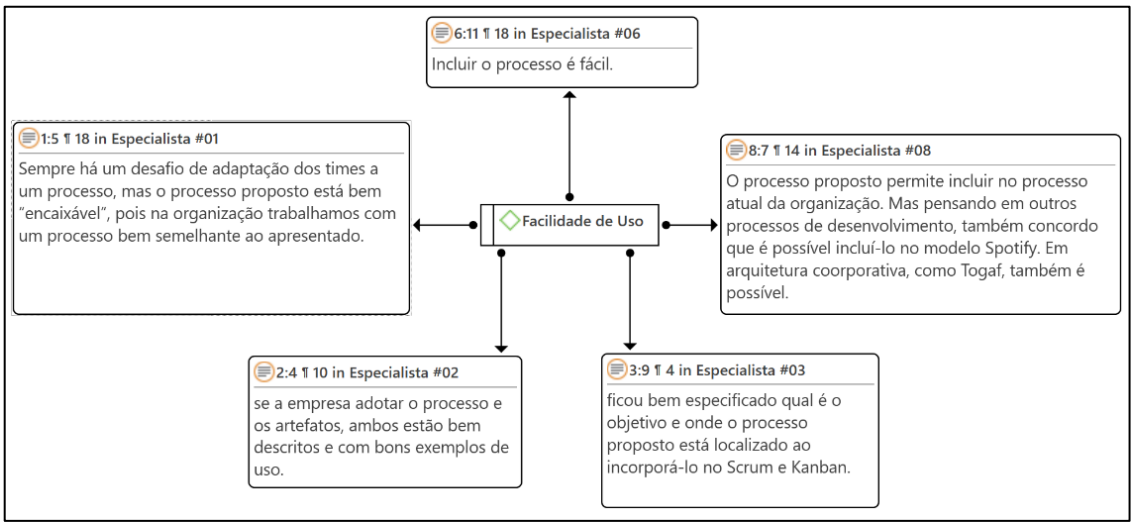

Figura 27. Rede com Associações à Codificação Facilidade de Uso.

O especialista #06, apenas se limitou a dizer que o processo é fácil de ser incluído no processo da organização em que atua. Os especialistas #02 e #04 relataram que o processo e os artefatos estão bem descritos e com bons exemplos de uso para integrá-los nos processos das organizações. O especialista #01 citou o desafio em adaptar os times ao novo processo, visto que conta com um novo papel e artefatos. No entanto, reconhece que esta evolução é normal e que o PDSOP é "bem encaixável" ao processo utilizado por eles. Por fim, o especialista #08 mencionou que mesmo em modelos conceituais para desenvolvimento de arquiteturas corporativas, como Togaf, o PDSOP pode ser incluído.

Em relação à Utilidade, a avaliação incide sobre a utilidade do processo, papel e artefatos propostos, analisando se são passíveis de serem adotados na indústria, com base nos princípios do TAM 3 (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008). A Figura 28 ilustra a rede associada à codificação Utilidade.

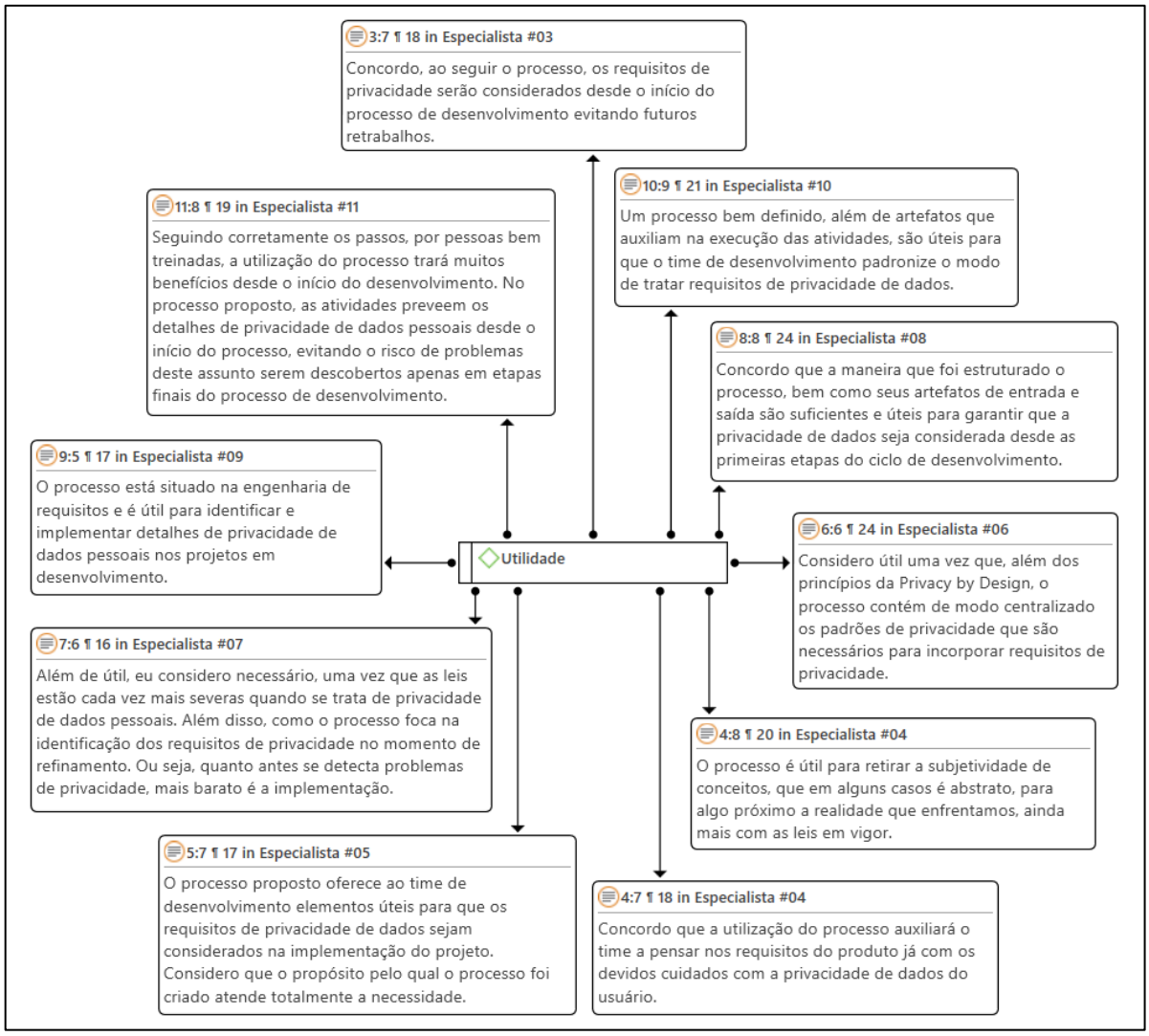

Figura 28. Rede com Associações à Codificação Utilidade.

Os especialistas #04, #05, #08, #09 e #11 mencionam que o processo, bem como os artefatos e o papel do Guardião de Privacidade, se seguidos corretamente, são úteis para implementar os requisitos de privacidade de dados desde as etapas iniciais do desenvolvimento de software, o que minimiza a possibilidade de descobrir problemas relacionados à privacidade serem descobertos apenas em fases mais tardias do processo, evitando o retrabalho por parte do time de desenvolvimento de software.

As questões de padronização das atividades relacionadas ao tratamento de dados pessoais foram citadas pelos especialistas #04, #06 e #10, os quais destacaram que o processo é útil, pois retira a subjetividade de como cada membro do time tratará questões relacionadas a privacidade de dados no projeto. Por fim, os

especialistas #04 e #07 citaram a utilidade do processo para auxiliar as organizações a estarem em conformidade com as novas leis sobre privacidade de dados pessoais.

O código Intenção de Uso Futuro, relacionado aos indícios positivos e negativos na implementação do processo nas organizações, é apresentado na Figura 29.

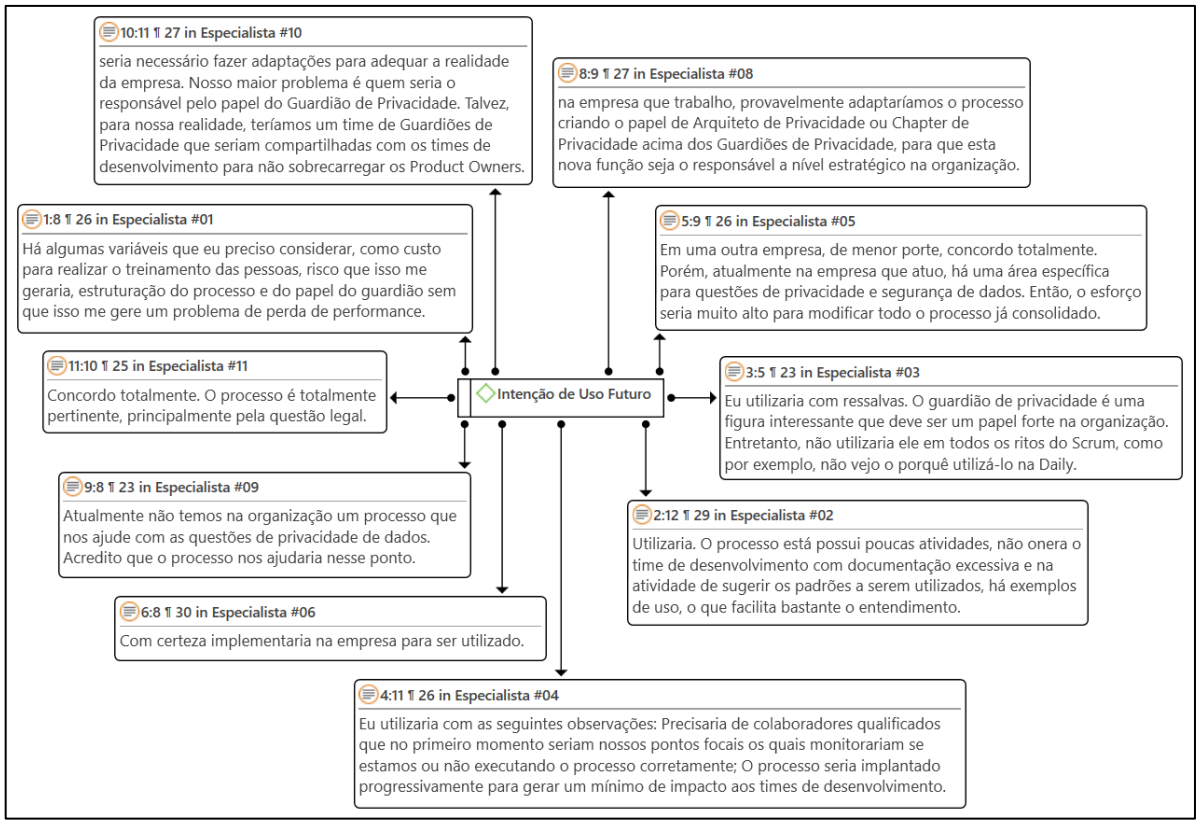

Figura 29. Rede com Associações à Codificação Intenção de Uso Futuro.

Os especialistas #02, #06, #9 e #11 mencionam a pertinência do processo, além de salientar que possuem intenção de implementar na organização. Opinião compartilhada pelos especialistas #01 e #04. Entretanto, estes últimos destacam algumas preocupações que devem ser consideradas, como o custo e treinamento de colaboradores para que a execução do processo siga conforme o esperado sem que os times de desenvolvimento tenham perda de performance.

Alguns especialistas citaram a intenção de utilizar o processo, porém, realizando adaptações para a realidade das organizações que atuam. O especialista #03 relatou que o Guardião de Privacidade, apesar de sua importância, poderia atuar de modo pontual em uma ou outra atividade do Scrum, e não em todos os ritos. O especialista #08 citou que na organização em que trabalha, seria interessante criar um novo papel, este, acima do Guardião de Privacidade, para atuar no nível

estratégico da organização, enquanto o Guardião de Privacidade atuaria, conforme o PDSOP, à nível de time de desenvolvimento. O especialista #10 mencionou que para a realidade da organização que atua, seria interessante criar um time de Guardiões de Privacidade para que estes atuem de modo compartilhado entre os times de desenvolvimento.

Apenas o especialista #05 relatou que não tem intenção de utilizar o processo na organização que atua, apesar de concordar que o PDSOP é útil e importante no tratamento de requisitos de privacidade durante o desenvolvimento de software. A justificativa se dá por atuar em uma organização de grande porte, na qual já existe um processo de desenvolvimento de software bem definido e o custo de adaptá-lo seria muito alto, inviabilizando o investimento.

O código Aspectos Positivos – Artefatos (Figura 30) visa compreender, na visão dos especialistas, quais são as vantagens da utilização dos artefatos propostos, tanto do Mapeamento entre Padrões de Privacidade e Princípios do *Privacy by Design* e o Repositório de Instâncias de Padrões de Privacidade.

Os especialistas #01, #02 e #03 relatam a utilidade e simplicidade dos artefatos propostos. Enfatizam, ainda, que houve êxito em apresentar exemplos simples e práticos de um assunto complexo e de difícil compreensão, que é a privacidade de dados pessoais e como aplicá-la no dia a dia de uma equipe de desenvolvimento. Ainda sobre a simplicidade dos artefatos, o especialista #10 ponderou que mesmo os profissionais com pouca experiência conseguem compreender como cada problema de privacidade pode ser resolvido e como cada padrão de privacidade pode auxiliar na solução.

O tempo de aprendizagem e soluções de problemas é outro fator determinante apontado pelos especialistas #05 e #09. Ambos mencionaram que os artefatos propostos, por fornecerem exemplos práticos e de fácil compreensão, reduzem o tempo de estudo e pesquisa do time de desenvolvimento ao encontrar a melhor solução para cada problema relacionado à privacidade de dados pessoais.

Por fim, os especialistas #06, #07, #09, #10 e #11 destacaram que os artefatos conseguiram abordar problemas reais de privacidade de dados enfrentados pelos times de desenvolvimento no dia a dia. Além disso, é possível atestar a utilização dos princípios fundamentais do *Privacy by Design* por meio da utilização dos padrões de privacidade, o que, segundo o especialista #10, pode ser útil em auditorias realizadas na organização.

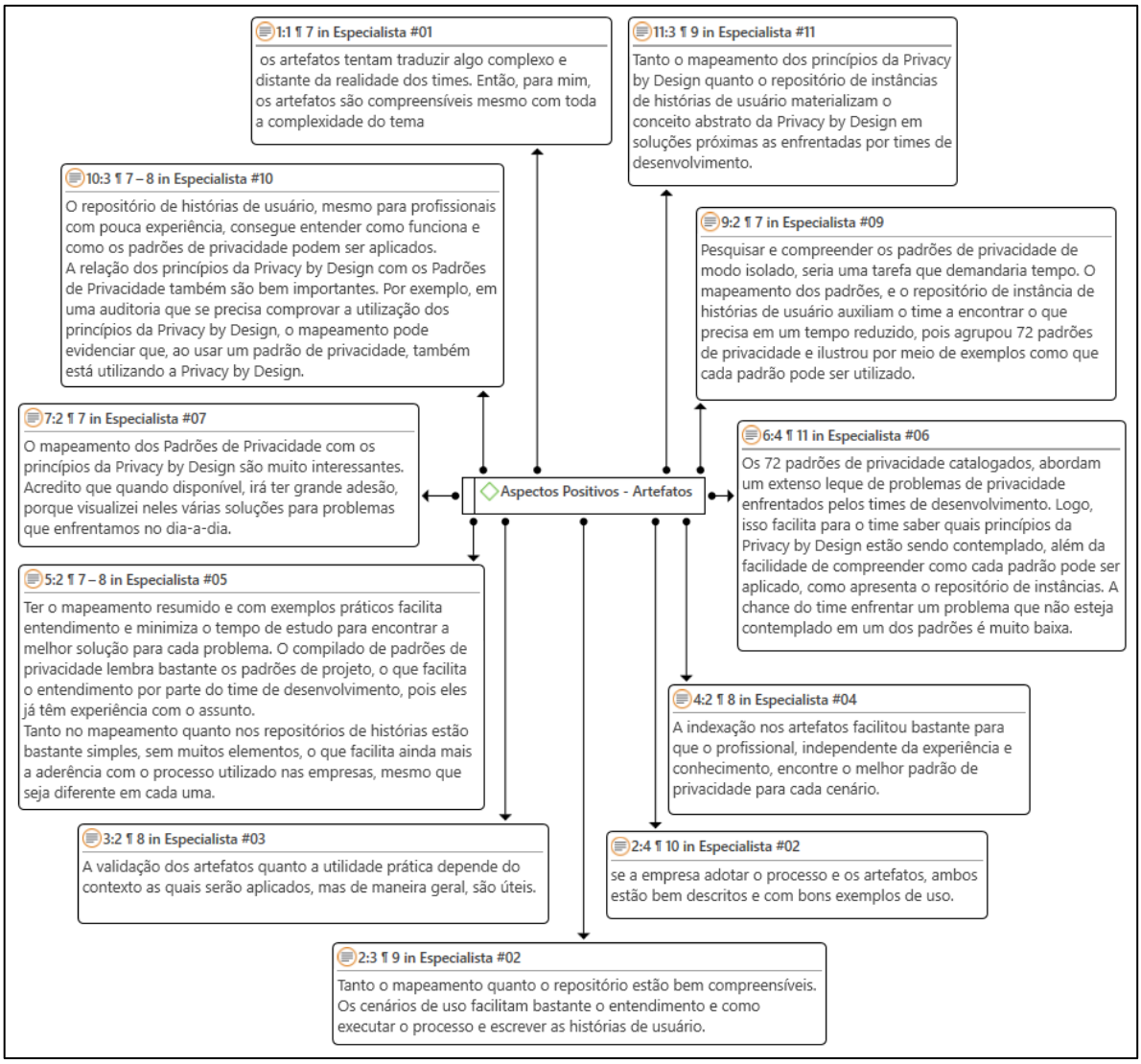

Figura 30. Rede com Associações à Codificação Aspectos Positivos - Artefatos.

O código Aspectos Positivos – Guardião de Privacidade compreende os pontos positivos referentes ao papel proposto, Guardião de Privacidade. A Figura 31 exibe a rede com associações à codificação citada.

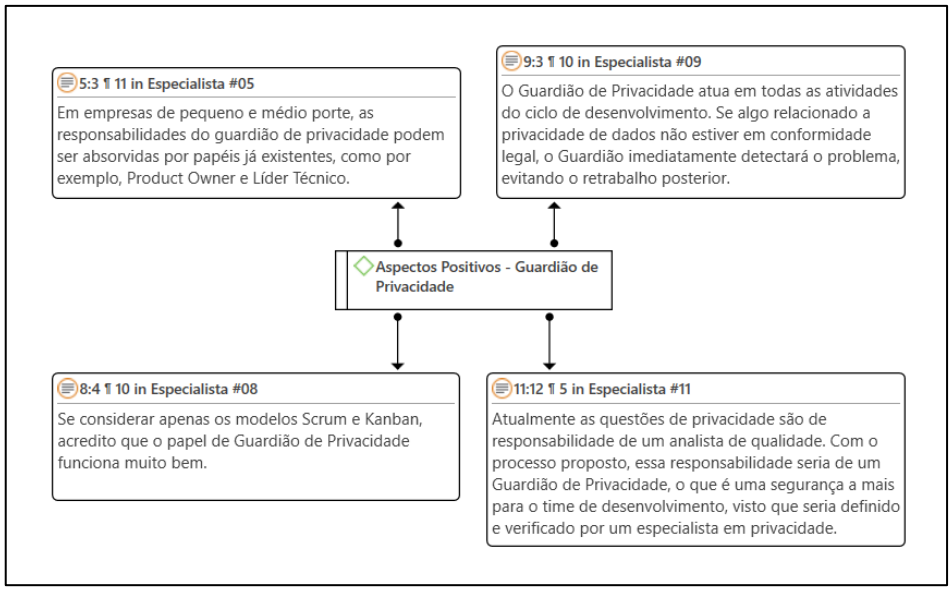

Figura 31. Rede com Associações à Codificação Aspectos Positivos - Guardião de Privacidade.

O especialista #05 mencionou que em organizações de pequeno e médio porte, as responsabilidades do Guardião de Privacidade podem ser absorvidas por profissionais que possuem outras funções no time de desenvolvimento, por exemplo, Product Owner e Líder Técnico. Isso pode ajudar a organização a economizar recursos, visto que não seria necessário a contratação de um colaborador específico para o papel de guardião.

O especialista #10, relatou que o papel do Guardião de Privacidade pode atuar muito bem nos processos ágeis de desenvolvimento. O especialista #09 enfatizou que o Guardião de Privacidade auxilia na detecção antecipada de problemas relacionados à privacidade e na eventual não conformidade legal que a organização possa ter, o que evitará o retrabalho futuro da equipe e eventuais multas em caso de descumprimento legal.

Por fim, o especialista #11 mencionou que o Guardião de Privacidade proporcionaria uma segurança a mais aos demais membros do time de desenvolvimento, pois os requisitos implementados por eles seriam definidos, revisados e validados por um profissional capacitado e especialista para tal atividade.

Em relação ao PDSOP, o código Aspectos Positivos – Processo contém as citações referentes aos pontos positivos na opinião dos especialistas e é ilustrado na Figura 32.

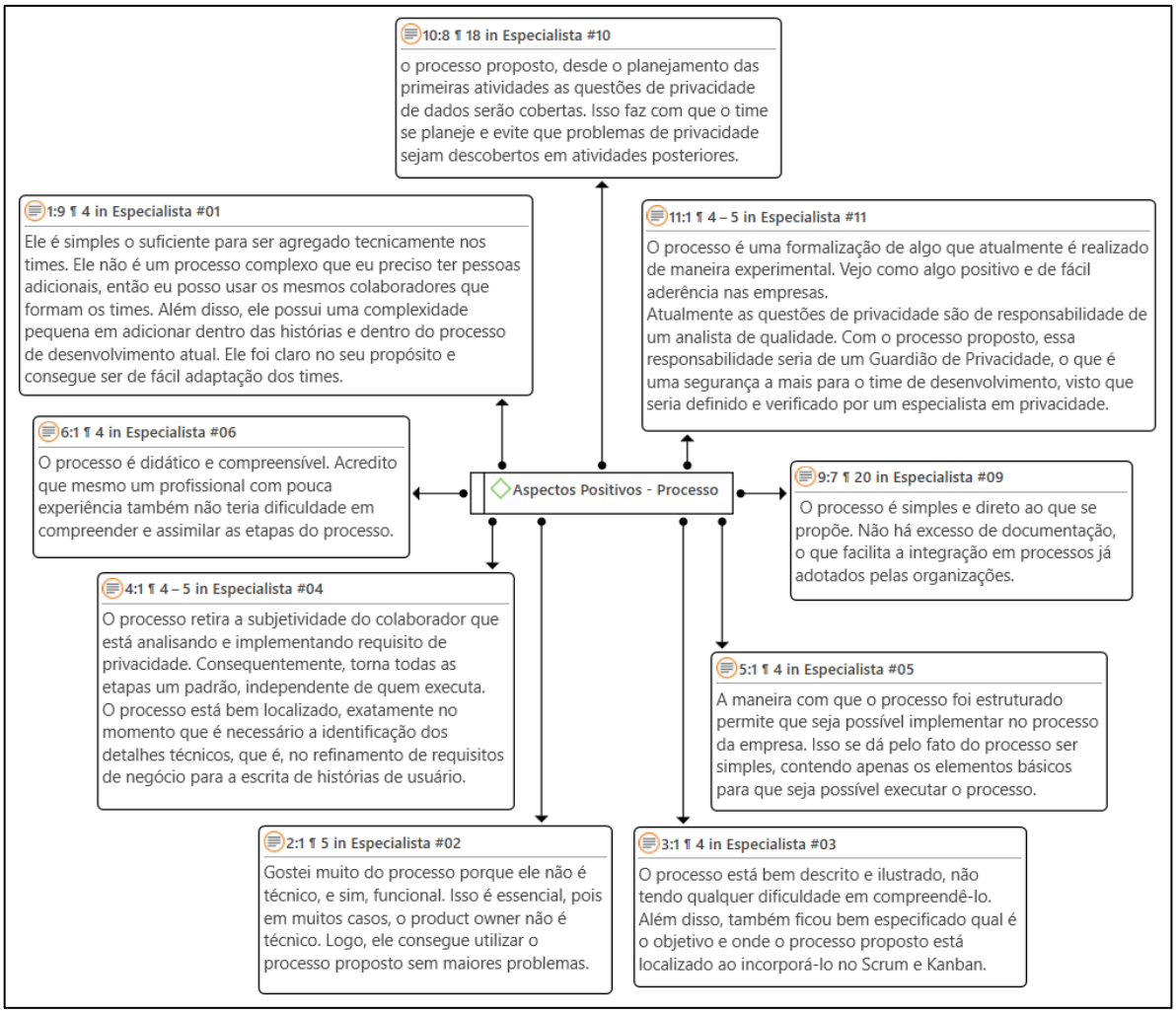

Figura 32. Rede com Associações à Codificação Aspectos Positivos - Processo.

Os especialistas #01, #03, #05, #09 e #11 mencionam a simplicidade do PDSOP, o que facilita incluí-lo ao processo atual das organizações sem gerar grandes mudanças. As principais características observadas pelos especialistas são a não sobrecarga do processo com documentações e a possibilidade de contar com um especialista em privacidade de dados em todos os times de desenvolvimento sem a necessidade de contratação de novos colaboradores apenas para assumir este papel.

Por sua vez, os especialistas #02 e #04 mencionaram que o processo é compreensível mesmo por colaboradores com pouca experiência e por Product Owners, que em algumas organizações não é um profissional técnico. Por fim, os especialistas #04 e #10 enfatizaram que o processo retira a subjetividade do colaborador responsável por tratar os requisitos de privacidade de dados pessoais. Desta maneira, independente do profissional, as etapas serão seguidas sistematicamente. Além disso, o cuidado com a privacidade de dados ocorre desde

as primeiras etapas de desenvolvimento o que reduz a possibilidade de ocorrerem problemas relacionados à privacidade de dados pessoais.

Além dos pontos positivos relacionados aos itens propostos (artefatos, papel do guardião de privacidade e processo), foram codificadas as suas limitações. A Figura 33 apresenta a rede de associações à codificação Limitações – Artefatos.

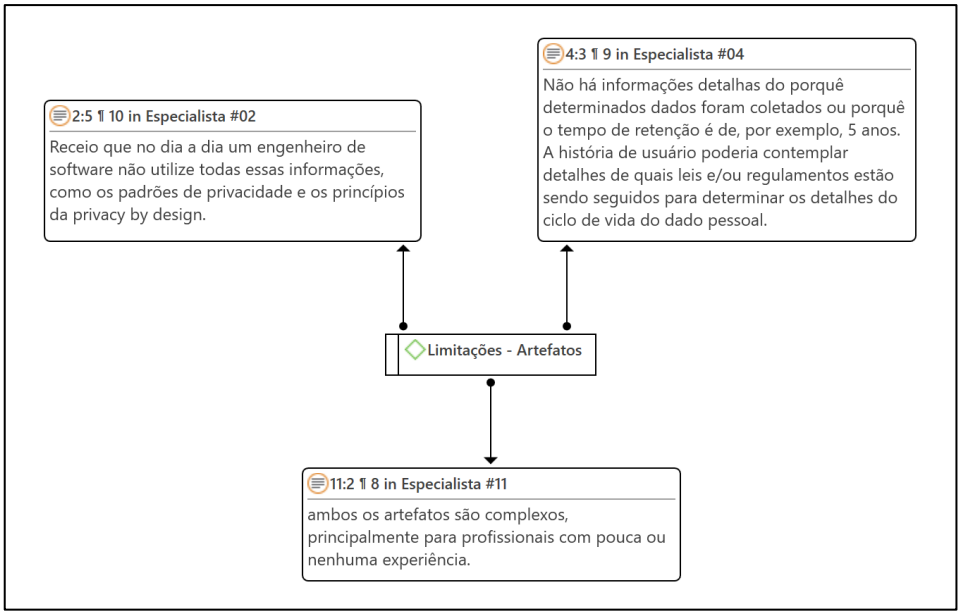

Figura 33. Rede com Associações à Codificação Limitações - Artefatos.

O especialista #02 mencionou a preocupação de que no dia a dia dos desenvolvedores de software, eles não façam uso dos artefatos e acabem utilizando outros meios para resolver os problemas relacionados à privacidade de dados pessoais.

O especialista #04 questionou a falta de detalhes do tempo de retenção utilizado em cada instância presente no artefato “Repositório de Instâncias de Padrões de Privacidade”. Na opinião dele, além da informação de quantos anos o dado pessoal ficará armazenado, a instância deverá apresentar a informação de quais leis e regulamentos foram considerados para definir o tempo de retenção dos dados pessoais.

Por fim, o especialista #11 cita a complexidade dos artefatos propostos, sendo de difícil utilização por parte de colaboradores com pouca ou nenhuma experiência em privacidade de dados pessoais.

O código Limitações – Guardião de Privacidade, apresentado na Figura 34, está relacionado com as limitações apontadas pelos especialistas no papel do Guardião de Privacidade.

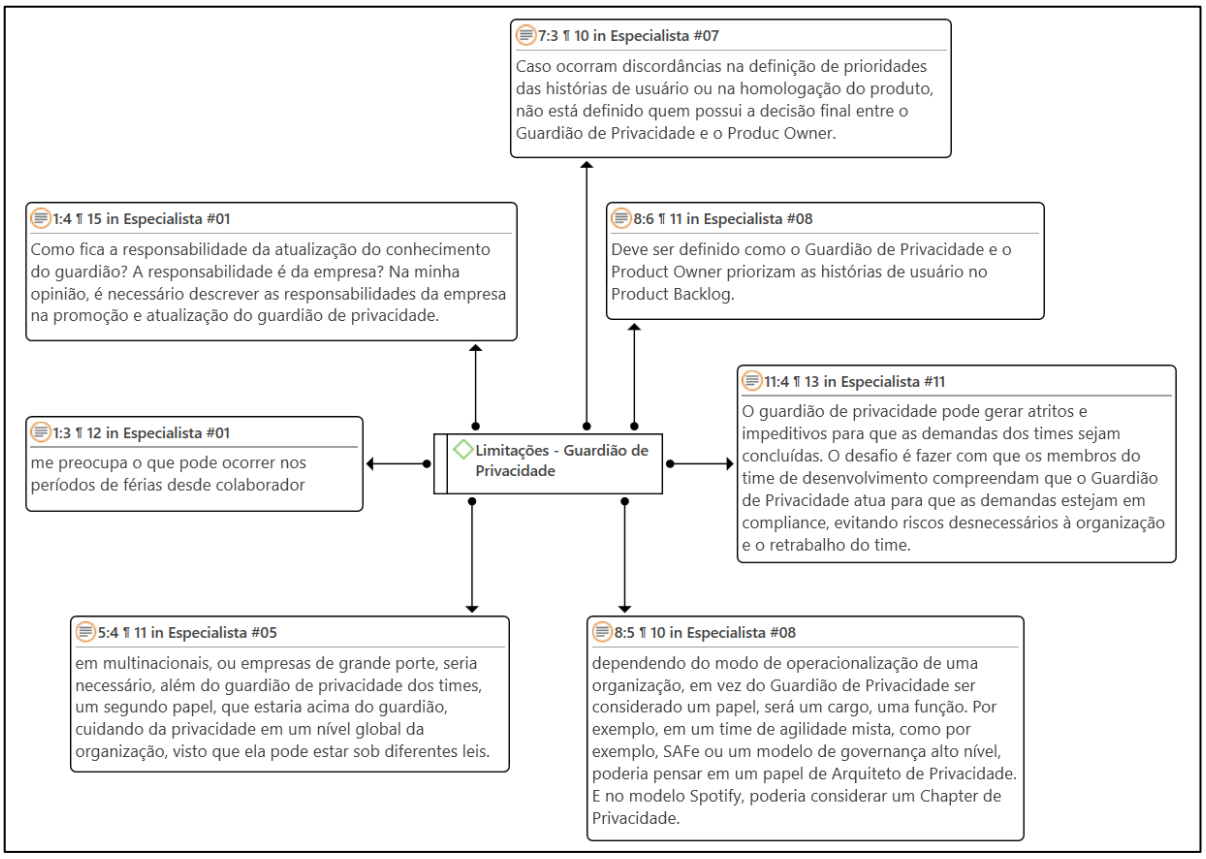

Figura 34. Rede com Associações à Codificação Limitações - Guardião de Privacidade.

Os especialistas #07, #08 e #11 apresentaram preocupações relacionadas aos atritos nos times de desenvolvimento, visto que em algumas ocasiões, as demandas dos times poderão sofrer atrasos por problemas relacionados à privacidade de dados, como relatado pelo especialista #11.

Por outro lado, os especialistas #07 e #08 mencionaram a preocupação com a hierarquia da organização, uma vez que não foi definido qual profissional terá a decisão final se for constatada discordâncias de opiniões na priorização de histórias de usuário ou homologação do produto.

Os especialistas #05 e #08 observaram que para organizações de grande porte, ou até mesmo multinacionais, seria necessário a criação de uma função acima do Guardião de Privacidade, por exemplo, um Arquiteto de Privacidade, o qual

gerenciaria os Guardiões de Privacidade que continuariam atuando nos times de desenvolvimento.

Por fim, o especialista #01 mencionou sobre a atualização do Guardião de Privacidade, uma vez que ele precisa se manter atualizado sobre leis e regulamentos da região que atua, bem como conhecer as novidades na área, como ferramentas, *frameworks* e tecnologias que podem ser empregadas no dia a dia do time de desenvolvimento. Além disso, o especialista #01 indagou sobre os períodos que o Guardião de Privacidade precisa se ausentar do time de desenvolvimento, seja por questões de saúde, férias ou atualizações.

No que se refere as limitações do processo, a Figura 35 apresenta a rede com associações à codificação Limitações – Processo.

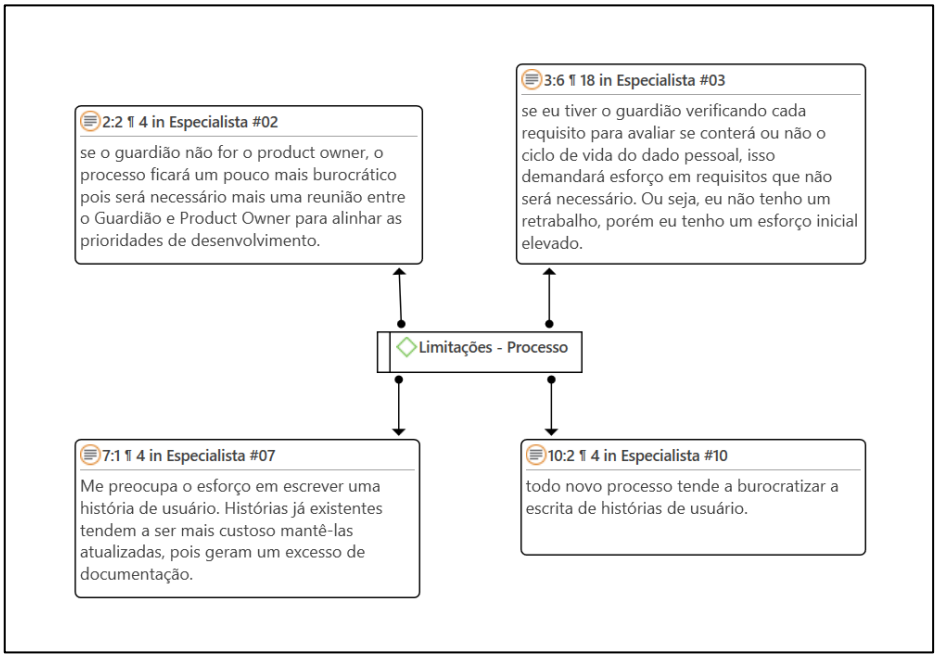

Figura 35. Rede com Associações à Codificação Limitações - Processo.

Houve preocupação dos especialistas quanto a burocratização do processo. Os especialistas #07 e #10 defenderam que todo novo processo inevitavelmente insere procedimentos os quais podem gerar excesso de documentação, enrijecendo e deixando o processo mais lento. O especialista #02 mencionou que se o Guardião de Privacidade e o Product Owner forem duas pessoas distintas, serão necessárias reuniões adicionais para chegarem em consenso sobre as prioridades das histórias de usuário. Por fim, o especialista #03 relatou que haverá um custo inicial para identificar se um determinado requisito manipulará dados pessoais.

A Figura 36 ilustra a rede com associações à codificação Recomendações de Uso. Os especialistas #05, #07 e #11, mencionaram que o PDSOP é relevante no contexto de privacidade de dados e recomendariam não apenas aos engenheiros de software, mas a outras áreas da organização em que atuam.

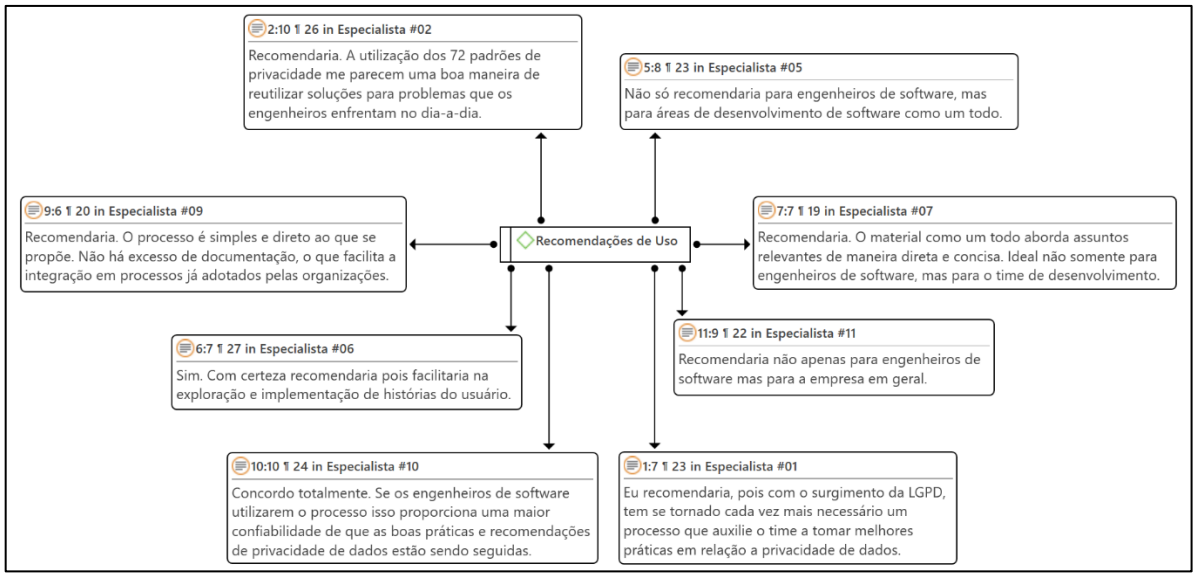

Figura 36. Rede com Associações à Codificação Recomendações de Uso.

Os especialistas #01 e #10, citaram que recomendariam o processo devido ao auxílio que proporciona aos times de desenvolvimento nas tomadas de decisões e no emprego de melhores práticas relacionadas à privacidade de dados pessoais. O especialista #01 ainda mencionou que isso se tornou ainda mais necessário devido à entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD).

Por fim, os especialistas #02, #06 e #09 relataram que recomendariam devido à facilidade do processo, tanto na execução quanto na integração aos processos das organizações em que atuam, pois não possui um excesso de documentação. O especialista #02 destacou os padrões de privacidade que, segundo ele, é uma boa maneira de reutilizar soluções para problemas enfrentados no dia a dia de engenheiros de software.

A última rede, diz respeito as sugestões de melhorias propostas pelos especialistas. A Figura 37 exibe a rede com associações à codificação Sugestões de Melhorias.

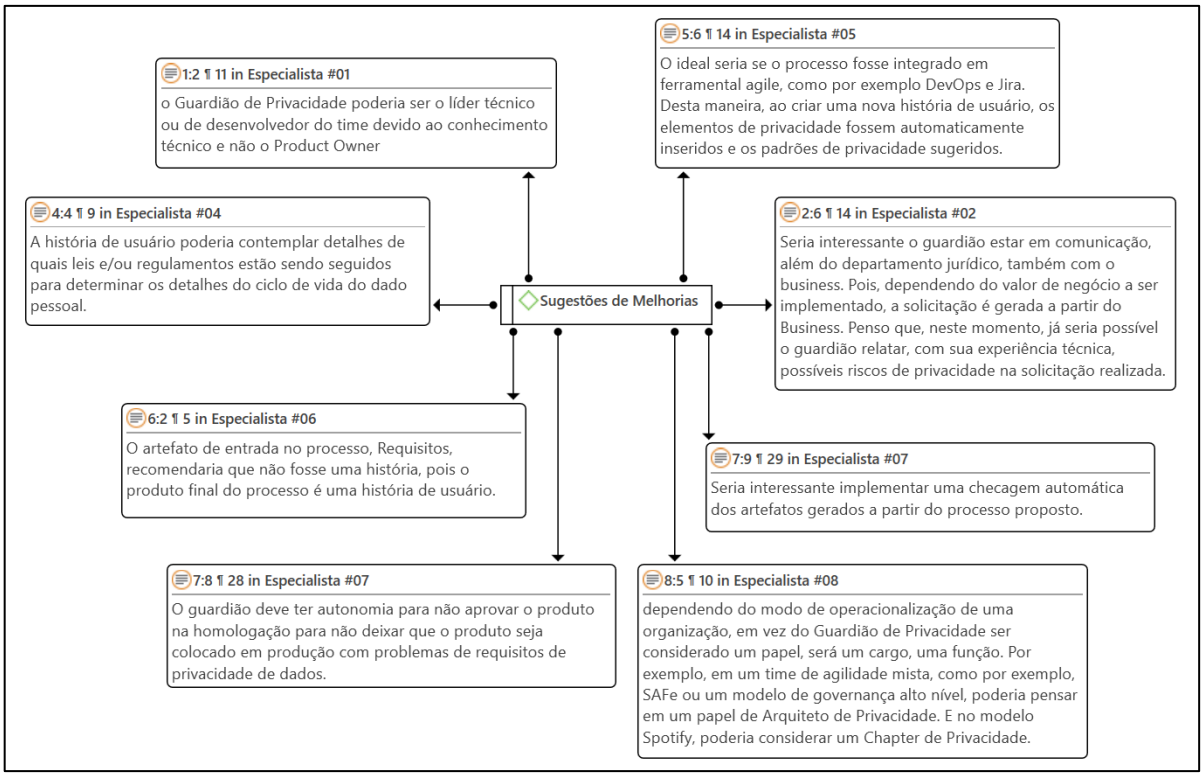

Figura 37. Rede com Associações à Codificação Sugestões de Melhorias.

Ao todo, oito sugestões foram propostas pelos especialistas. O especialista #01 mencionou que o papel do Guardião de Privacidade pudesse ser absorvido pelo líder técnico ou um desenvolvedor do time, visto o conhecimento técnico que esses colaboradores possuem.

O especialista #07 citou que a homologação do produto deve ter a anuência do Guardião de Privacidade. Desta maneira, minimizam-se as chances de problemas de requisitos de privacidade serem descobertos em ambiente de produção.

A recomendação sugerida pelo especialista #02 está relacionada à comunicação do Guardião de Privacidade com o departamento de Marketing da organização. Pois, segundo ele, há demandas que partes do Marketing e não dos usuários. Consequentemente, neste momento o Guardião de Privacidade pode intervir e mitigar futuros problemas relacionados à privacidade de dados pessoais.

Em relação ao PDSOP, o especialista #06 relatou que o artefato de entrada da atividade “Identificar a Necessidade de Ciclo de Vida do Dado Pessoal” não fosse uma história de usuário que precisa ser refinada, e sim um épico ou uma *feature* a qual necessita ser desdobrada em unidades de trabalho menores.

Os especialistas #05 e #07 sugeriram que o PDSOP fosse integrado com ferramentas utilizadas pelas organizações para gestão de projetos ágeis, como

DevOps e Jira. Desta maneira, a escrita de história de usuário contemplando restrições de privacidade de dados pessoais seria automatizada.

Por fim, o especialista #08 mencionou que o PDSOP poderia ser adaptado para modelos de governança de alto nível, por exemplo, SAFe (*Scaled Agile Framework*).

7.3 Discussões

Esta seção apresenta as discussões relacionadas aos resultados obtidos por meio das avaliações dos 11 (onze) especialistas e está organizada conforme as codificações obtidas após o processo de Codificação Provisória (SALDAÑA, 2013).

Facilidade de Uso

Enquanto o Especialista #06 expressou uma opinião geral positiva, afirmando que o processo é fácil de ser incluído nas práticas organizacionais, outros especialistas ofereceram sugestões mais detalhadas. Os especialistas #02 e #04 destacaram a clareza e a qualidade da descrição do processo, bem como a presença de exemplos práticos que facilitam a integração do processo e seus artefatos nas operações das organizações. Isso indica que a documentação abrangente e os exemplos relevantes desempenham um papel significativo na percepção da facilidade de uso pelos usuários.

Por outro lado, o Especialista #01 levantou um desafio importante relacionado à adaptação das equipes ao novo processo, especialmente devido à introdução de um novo papel e artefatos. No entanto, ele reconhece que essa resistência é parte natural do processo de evolução e observa que o PDSOP se encaixa bem no contexto organizacional existente. Esse comentário ressalta a importância não apenas da usabilidade do processo em si, mas também da consideração dos aspectos organizacionais e culturais durante a implementação.

Um ponto adicional foi levantado pelo Especialista #08, que destacou a versatilidade do PDSOP ao sugerir sua inclusão em modelos conceituais mais amplos, como o TOGAF. Isso sugere que o processo proposto não apenas é fácil de ser adotado dentro de uma organização específica, mas também possui potencial para integração em estruturas mais abrangentes de gerenciamento e desenvolvimento de sistemas.

Utilidade

Em relação a Utilidade dos elementos do processo proposto, incluindo artefatos e o papel do Guardião de Privacidade, as opiniões dos especialistas revelam uma percepção positiva entre os entrevistados. Os especialistas #04, #05, #08, #09 e #11, destacaram a utilidade desses componentes para a implementação eficaz dos requisitos de privacidade de dados desde as etapas iniciais do desenvolvimento de software. Esta observação é crucial, pois sugere que o processo não apenas aborda questões de privacidade, mas também o faz de forma proativa, reduzindo a probabilidade de problemas relacionados à privacidade surgirem em fases posteriores do desenvolvimento. Isso pode resultar em economia de tempo e recursos, minimizando o retrabalho e aumentando a eficiência do processo de desenvolvimento de software.

Além disso, os especialistas #04, #06 e #10 destacaram a utilidade do processo na padronização das atividades relacionadas ao tratamento de dados pessoais para garantir consistência e eliminar a subjetividade na forma como diferentes membros da equipe tratam as questões de privacidade de dados durante o projeto. Essa observação ressalta a importância de ter diretrizes claras e consistentes para garantir a conformidade e a eficácia no tratamento de dados sensíveis.

Por fim, os especialistas #04 e #07 mencionaram a utilidade do processo para auxiliar as organizações a estarem em conformidade com as novas leis sobre privacidade e proteção de dados pessoais. Esta observação é especialmente relevante em um contexto em que as regulamentações de privacidade estão se tornando cada vez mais rigorosas e as organizações enfrentam desafios crescentes em garantir conformidade com essas leis em constante evolução. Portanto, o reconhecimento da utilidade do processo nesse aspecto indica que ele pode servir como uma ferramenta valiosa para ajudar as organizações a atenderem às suas obrigações legais e a protegerem a privacidade dos dados de seus clientes e usuários.

Intenção de Uso Futuro

No que diz respeito a codificação de Intenção de Uso Futuro, os especialistas expressaram uma intenção positiva de adotar o PDSOP, destacando sua pertinência e importância para lidar com os requisitos de privacidade desde as fases iniciais do desenvolvimento de software.

Os especialistas #02, #06, #09, #11, #01 e #04 demonstraram uma clara intenção de implementar o processo em suas organizações. No entanto, alguns deles, como os especialistas #01 e #04, também levantaram preocupações legítimas relacionadas ao custo e ao treinamento de colaboradores. Essas preocupações destacam a importância de considerar não apenas a utilidade percebida do processo, mas também os recursos necessários para sua implementação eficaz, incluindo investimentos em treinamento e capacitação dos colaboradores.

Além disso, alguns especialistas expressaram uma intenção de usar o processo, mas sugeriram adaptações específicas para se adequarem melhor à realidade de suas organizações. Por exemplo, o especialista #03 sugeriu uma abordagem mais flexível para o papel do Guardião de Privacidade, permitindo sua atuação em atividades específicas do Scrum, em vez de em todos os ritos. Da mesma forma, o especialista #08 propôs a criação de um novo papel acima do Guardião de Privacidade, para lidar com questões estratégicas, enquanto o Guardião de Privacidade permaneceria em nível operacional. Essas sugestões ressaltam a importância da adaptabilidade do processo para atender às necessidades específicas de cada organização.

Por outro lado, o especialista #05 foi o único a expressar uma falta de intenção em utilizar o processo em sua organização. Sua justificativa foi baseada no fato de que a organização em que atua, possuir um processo de desenvolvimento de software bem estabelecido e os custos de adaptação seriam proibitivos. Essa observação destaca a importância de considerar o contexto organizacional e as limitações existentes ao decidir sobre a implementação de novos processos.

Portanto, há uma disposição positiva dos especialistas em adotar o PDSOP. Porém, deve-se destacar a necessidade de considerar cuidadosamente as preocupações e sugestões levantadas por eles para garantir uma implementação eficaz e bem-sucedida do processo em suas organizações.

Aspectos Positivos – Artefatos

As avaliações relativas ao código Aspectos Positivos – Artefatos revelam as vantagens percebidas pelos especialistas em relação aos artefatos propostos, que foram amplamente reconhecidos pelos especialistas como úteis, simples de entender e eficazes na abordagem de problemas reais relacionados à privacidade de dados pessoais.

Os especialistas #01, #02 e #03 elogiaram a capacidade dos artefatos em apresentar exemplos simples e práticos de conceitos complexos, como a privacidade de dados pessoais e sua aplicação no contexto do desenvolvimento de software. Esse reconhecimento sugere que os artefatos são eficazes em tornar conceitos complexos mais acessíveis e compreensíveis para os membros da equipe, independentemente do nível de experiência.

Por outro lado, os especialistas #05 e #09 destacaram a capacidade dos artefatos propostos em reduzir o tempo necessário para o estudo e pesquisa relacionados à privacidade de dados pessoais, o que leva a uma maior produtividade e eficácia no tratamento de questões relacionadas à privacidade durante o desenvolvimento de software. Por fim, os especialistas #06, #07, #09, #10 e #11 destacaram que os artefatos conseguiram abordar problemas reais enfrentados pelas equipes de desenvolvimento no dia a dia.

Deste modo, as avaliações realizadas pelos especialistas indicam que os artefatos propostos são amplamente reconhecidos como valiosos e eficazes. Sua utilidade, simplicidade, capacidade de reduzir o tempo de aprendizagem e pesquisa, bem como sua capacidade de abordar problemas reais e aplicar os princípios do PbD, os tornam recursos essenciais para a integração da privacidade de dados no desenvolvimento de software.

Aspectos Positivos – Guardião de Privacidade

O especialista #05 apontou que em empresas de pequeno e médio porte, as responsabilidades do Guardião de Privacidade podem ser incorporadas por profissionais que já desempenham outras funções no time de desenvolvimento. Isso indica uma adaptação flexível do papel do Guardião de Privacidade de acordo com as

necessidades e recursos disponíveis da organização, proporcionando economia de recursos ao evitar a contratação de um colaborador específico para esse papel.

Por outro lado, o especialista #09 enfatizou que o Guardião de Privacidade desempenha um papel crucial na detecção antecipada de problemas relacionados à privacidade e na garantia da conformidade legal da organização. Essa observação destaca a importância do papel do Guardião de Privacidade na identificação proativa de riscos e na mitigação de possíveis não conformidades legais, contribuindo assim para evitar retrabalho futuro e possíveis multas decorrentes de descumprimento legal.

Por fim, o especialista #11 ressaltou que o Guardião de Privacidade proporciona uma camada adicional de segurança aos demais membros do time de desenvolvimento. Isso ocorre porque os requisitos implementados são definidos, revisados e validados por um profissional especializado e capacitado, garantindo assim a integridade e conformidade dos requisitos relacionados à privacidade de dados. Essa validação contribui para aumentar a confiança na implementação e reduzir o risco de falhas de segurança ou não conformidades.

Com isso, os resultados destacam a importância e eficácia do papel do Guardião de Privacidade no processo proposto, evidenciando sua capacidade de adaptar-se a diferentes contextos organizacionais, integrar-se a metodologias ágeis, garantir a conformidade legal e reforçar a segurança e validade dos requisitos implementados relacionados à privacidade e proteção de dados pessoais.

Aspectos Positivos – Processo

O código Aspectos Positivos – Processo refere-se às vantagens percebidas pelos especialistas em relação ao PDSOP. Os especialistas #01, #03, #05, #09 e #11 ressaltaram a simplicidade do processo proposto, destacando que sua implementação não requer grandes mudanças nos processos existentes nas organizações. Desta maneira, pode-se concluir que o processo pode ser facilmente incorporado ao fluxo de trabalho existente, simplificando sua adoção e minimizando qualquer interrupção nas operações.

Os especialistas #02, #04 e #10 destacaram a compreensibilidade do processo, mesmo para colaboradores com pouca experiência e para Product Owners que podem não ser profissionais técnicos em algumas organizações. Essa observação

indica que o processo oferece diretrizes claras e objetivas, eliminando ambiguidades e garantindo consistência na abordagem da privacidade de dados.

Da mesma maneira, os especialistas #04 e #10 também destacaram que o processo se preocupa com a privacidade de dados desde as primeiras etapas de desenvolvimento, reduzindo assim a possibilidade de ocorrerem problemas relacionados à privacidade de dados. Essa observação enfatiza a importância da integração da privacidade desde o início do ciclo de vida do desenvolvimento de software, contribuindo para a mitigação de riscos e a garantia de conformidade com regulamentos de privacidade.

Isto posto, os resultados do código de aspectos positivos referentes ao processo indicam que o processo proposto é percebido como simples, compreensível e eficaz na abordagem da privacidade de dados. Sua capacidade de facilitar a integração nas organizações, eliminar a subjetividade no tratamento dos requisitos de privacidade e garantir o cuidado com a privacidade e proteção de dados pessoais desde as etapas iniciais do desenvolvimento faz com que o processo possua um potencial significativo para ser adotado e utilizado no futuro pelas organizações de desenvolvimento de software.

Limitações – Artefatos

Em relação às limitações dos artefatos propostos, o especialista #02 expressou preocupação de que os desenvolvedores de software possam não fazer uso dos artefatos propostos no seu dia a dia. Para abordar essa preocupação, foi desenvolvido um repositório de informações que utiliza filtros por palavras-chave para auxiliar os desenvolvedores a encontrar soluções adequadas para os problemas de privacidade e proteção de dados. Essa abordagem visa facilitar o acesso e a utilização dos artefatos pelos desenvolvedores, aumentando sua efetividade e adoção.

O especialista #04 questionou a falta de detalhes sobre o tempo de retenção utilizado em cada instância presente no artefato "Repositório de Instâncias de Padrões de Privacidade". Ele destacou a importância de incluir informações sobre quais leis e regulamentos foram considerados para definir o tempo de retenção dos dados pessoais. Em resposta a essa preocupação, o artefato foi revisado e um novo campo denominado "Leis e Regulamentos" foi adicionado às histórias de usuário geradas a partir do processo. Isso permitirá que o Guardião de Privacidade insira informações

relevantes sobre as leis e regulamentos que impactam cada instância, melhorando a transparência e a conformidade do processo.

Por fim, o especialista #11 mencionou a complexidade dos artefatos propostos, observando que podem ser difíceis de utilizar para colaboradores com pouca ou nenhuma experiência em privacidade de dados. Em resposta a essa preocupação, os artefatos foram revisados e simplificados, reduzindo a quantidade de informações apresentadas. Apenas as informações pertinentes ao contexto, problema e solução, juntamente com um exemplo de uso são apresentados no repositório de informações. Essa simplificação visa tornar os artefatos mais acessíveis e compreensíveis para uma variedade de usuários, independentemente do seu nível de experiência.

Com isso, os resultados destacam a importância de abordar preocupações específicas dos especialistas relacionadas à utilização e detalhamento dos artefatos propostos. As revisões e adaptações feitas nos artefatos em resposta a essas preocupações visam melhorar sua eficácia, acessibilidade e utilidade para os usuários, contribuindo assim para o sucesso geral do processo proposto.

Limitações – Guardião de Privacidade

A análise dos resultados do código referentes às limitações do papel do Guardião de Privacidade revela preocupações levantadas pelos especialistas em relação aos desafios e responsabilidades associados a esse papel. Os especialistas #07, #08 e #11 expressaram preocupações sobre possíveis atritos nos times de desenvolvimento decorrentes de atrasos nas demandas causados por problemas relacionados à privacidade de dados. Em resposta a essa preocupação, as responsabilidades do Guardião de Privacidade foram atualizadas para incluir a proposta e ministração de cursos de privacidade de dados aos demais membros da equipe. Isso visa capacitar e conscientizar a equipe sobre a importância da privacidade de dados nos projetos de software, ajudando a reduzir atritos e a melhorar a colaboração.

Os especialistas #07 e #08 mencionaram preocupações sobre a hierarquia da organização e a falta de definição sobre qual profissional terá a decisão final em casos de discordância na priorização de histórias de usuário ou na homologação do produto. O processo proposto não interfere no modelo de gestão do time de desenvolvimento, deixando a responsabilidade de priorização de histórias de usuário ao Product Owner,

caso a organização utilize o Scrum. Essa abordagem visa garantir que as atividades do processo respeitem o modelo de gestão e as práticas já estabelecidas na organização, minimizando conflitos e garantindo uma operação eficiente.

Os especialistas #05 e #08 observaram que empresas de grande porte podem necessitar de uma função superior ao Guardião de Privacidade, como um Arquiteto de Privacidade, para gerenciar os Guardiões de Privacidade que atuam nos times de desenvolvimento. Isso sugere uma adaptação do processo proposto para tratar com as complexidades e necessidades específicas de empresas de grande porte, o que pode ser considerado como trabalhos futuros (Seção 8.4). Essa adaptação exigirá novos estudos de caso para compreender como os requisitos de privacidade de dados são tratados em organizações desse porte.

O especialista #01 destacou a importância da atualização contínua do Guardião de Privacidade sobre leis, regulamentos e novidades na área de privacidade e proteção de dados pessoais. Isso inclui a necessidade de se ausentar do time de desenvolvimento para participar de cursos e atualizações. Para esta questão, as responsabilidades do Guardião de Privacidade foram atualizadas, estabelecendo que a organização deve promover cursos internos para garantir que ao menos dois membros da equipe tenham o conhecimento necessário para suprir ausências pontuais do profissional.

Em resumo, os resultados referentes às limitações do papel do Guardião de Privacidade destacam a importância de abordar preocupações específicas dos especialistas para garantir uma implementação eficaz e bem-sucedida do papel no processo proposto. As atualizações e adaptações feitas em resposta a essas preocupações visam melhorar a colaboração, garantir a conformidade e abordar os desafios específicos enfrentados por diferentes tipos e tamanhos de organizações.

Limitações – Processo

Referente às limitações do processo, pode-se destacar preocupações específicas dos especialistas relacionadas à possível burocratização do processo proposto e aos desafios associados à identificação e tratamento de requisitos de privacidade de dados, conforme apontado pelos especialistas #07 e #10. Para esta preocupação, o processo proposto foi concebido para auxiliar as equipes a projetar softwares com foco em privacidade de dados desde as etapas iniciais do

desenvolvimento. Além disso, foi proposto que o artefato de saída seja apenas uma história de usuário que inclua critérios de privacidade de dados, eliminando a necessidade de documentação adicional e minimizando a burocracia.

O especialista #02 mencionou a necessidade de consenso entre o Guardião de Privacidade e o Product Owner, caso sejam pessoas distintas. Ele destacou que essa situação pode exigir reuniões adicionais. Embora as responsabilidades do Guardião de Privacidade possam ser absorvidas pelo Product Owner, recomenda-se que sejam dois colaboradores distintos para garantir uma abordagem abrangente, evitar conflitos de interesse e negligências em problemas relacionados à privacidade e proteção de dados pessoais.

Para o especialista #03 há um custo inicial associado à identificação de requisitos que envolvem dados pessoais. Entretanto, esta atividade é de extrema importância para minimizar os riscos do projeto, pois problemas de privacidade de dados identificados tardiamente podem ser mais custosos de serem corrigidos. Além disso, o não cumprimento da legislação pode acarretar multas para a organização.

Desta maneira, os resultados das limitações referentes ao processo destacam desafios significativos relacionados à burocratização, consenso entre os envolvidos e custos iniciais de identificação de requisitos de privacidade de dados. As adaptações e sugestões feitas em resposta a essas preocupações visam minimizar os impactos negativos, garantir uma abordagem eficaz da privacidade de dados e promover o sucesso do processo proposto.

Recomendações de Uso

Os especialistas #05, #07 e #11 ressaltaram sua relevância não só para engenheiros de software, mas para toda a organização, destacando sua utilidade em diversos setores. Os especialistas #01 e #10 enfatizaram como o processo auxilia os times de desenvolvimento na tomada de decisões e na adoção de melhores práticas, especialmente diante da Lei Geral de Proteção de Dados Pessoais (LGPD). Por sua vez, os especialistas #02, #06 e #09 elogiaram a facilidade de execução e integração do processo aos fluxos organizacionais existentes, destacando a ausência de excesso de documentação e a facilidade de implementação prática. Além disso, o especialista #02 destacou a vantagem da reutilização de padrões de privacidade, observando que

isso proporciona eficiência e consistência na abordagem de questões de privacidade de dados.

Sendo assim, os resultados das recomendações de uso destacam a percepção positiva dos especialistas em relação à relevância, utilidade e facilidade de integração do processo proposto em diferentes contextos organizacionais. As recomendações ressaltam a importância do processo como uma ferramenta eficaz para lidar com os desafios da privacidade de dados e garantir a conformidade com regulamentações, ao mesmo tempo em que facilita a execução e a integração com os fluxos de trabalho existentes.

Sugestões de Melhorias

As recomendações de melhorias do PDSOP feitas pelos especialistas forneceram sugestões para aprimorar diferentes aspectos do processo, desde a distribuição de responsabilidades até a integração com ferramentas e modelos de governança de alto nível.

O especialista #01 recomendou que o papel do Guardião de Privacidade pudesse ser absorvido pelo líder técnico ou um desenvolvedor do time, dado o conhecimento técnico desses colaboradores. Essa sugestão foi acatada e o papel do Guardião de Privacidade foi atualizado para incluir menções aos colaboradores que poderiam receber essas responsabilidades. Isso permite uma distribuição mais flexível de tarefas, adaptando-se às habilidades e responsabilidades dos membros da equipe.

Por outro lado, o especialista #07 sugeriu que a homologação do produto incluísse a anuência do Guardião de Privacidade, minimizando a descoberta de problemas de privacidade de dados em ambiente de produção. Essa recomendação foi aceita e as definições do Guardião de Privacidade foram atualizadas para garantir sua participação nesse processo, mesmo que isso implique em reuniões adicionais para garantir uma abordagem abrangente da privacidade de dados.

Sob outro ponto de vista, o especialista #04 propôs que as histórias de usuário incluíssem detalhes sobre as leis e regulamentos seguidos para determinar o ciclo de vida dos dados pessoais. Essa sugestão foi implementada e o artefato gerado a partir do processo foi atualizado para incluir essa informação, proporcionando uma visão mais completa e transparente dos requisitos de privacidade de dados.

Os especialistas #05 e #07 sugeriram a integração do processo proposto com ferramentas de gestão de projetos ágeis, como DevOps e Jira, para automatizar a escrita de histórias de usuário que abordem restrições de privacidade de dados. Essa sugestão destaca a importância de tornar o processo mais eficiente e integrado aos fluxos de trabalho existentes. No entanto, a implementação de *plugins* com a finalidade de integrar o processo às ferramentas citadas serão desenvolvidas como trabalhos futuros.

Por fim, o especialista #08 mencionou que o processo proposto poderia ser adaptado para modelos de governança de alto nível, como o SAFe *(Scaled Agile Framework)*. Essa sugestão destaca a necessidade de flexibilidade e adaptação do processo para atender às demandas e estruturas organizacionais específicas, garantindo sua aplicabilidade em diferentes contextos. Trabalhos futuros abordarão também essa lacuna, a fim de propor adaptações específicas aos modelos escaláveis, como SAFe.

As contribuições dos 11 (onze) especialistas neste projeto desempenharam um papel fundamental no aprimoramento da instrumentação do estudo e no contínuo refinamento do processo, papel e artefatos produzidos. Por meio dessas melhorias o processo foi aprimorado para facilitar a adaptação e possibilitar sua aplicação em futuros projetos industriais.

7.4 Ameaças à Validade da Avaliação

Ameaças à validade de constructo. Realizaram-se diversas reuniões entre os pesquisadores participantes com o intuito de discutir e validar os instrumentos utilizados na avaliação do processo, papel e artefatos propostos.

Ameaças à validade interna. Para mitigar essa ameaça, a amostra foi composta por especialistas com diferentes perfis, como nível de formação, cargo/função que exercem, anos de experiência, e organizações de diferentes portes e domínios. Adicionalmente, esta ameaça foi tratada assegurando que as identidades dos especialistas fossem mantidas em sigilo e que todos os materiais produzidos fossem anonimizados. Dessa forma, foi proporcionado um ambiente em que os especialistas se sentissem à vontade para expressar suas opiniões sem receio de possíveis inconvenientes futuros, e as respostas foram significantes para melhorar todos os artefatos avaliados neste estudo.

Ameaças à validade externa. A obtenção de especialistas com conhecimento e experiência em privacidade de dados e processos de desenvolvimento de software foi uma das grandes dificuldades para a condução desta avaliação. Devido ao pequeno número de participantes envolvidos no estudo qualitativo (N = 11), não se pode assegurar a generalização dos resultados apresentados. Contudo, buscou-se mitigar essa limitação ao realizar a pesquisa com especialistas com experiências distintas, provenientes de diversas organizações e ocupando diversos cargos/funções.

Ameaças à validade de resposta. A presença do pesquisador durante a entrevista pode influenciar as respostas do avaliador devido a diversos fatores, como comportamento, linguagem corporal, sugestões inadvertidas, entre outros. Entretanto, esta limitação foi mitigada por meio da padronização do protocolo de pesquisa, em que apenas as afirmações presentes no instrumento de pesquisa eram lidas ao avaliador e justificativas eram solicitadas em momentos oportunos, sempre mantendo uma postura neutra sobre a avaliação.

Ameaças à validade de conclusão. A principal limitação foi a quantidade de especialistas (N = 11). Contudo, é importante destacar que o conhecimento e a experiência desses especialistas desempenharam um papel significativo na qualidade desta avaliação, considerando sua natureza qualitativa. Embora um número maior de especialistas pudesse aumentar a capacidade de generalização dos resultados, as contribuições dos participantes existentes foram valiosas para a qualidade geral da pesquisa.

7.5 Considerações sobre o Capítulo

Neste capítulo foi apresentada a avaliação do PDSOP, por especialistas em privacidade de dados pessoais e processos de desenvolvimento de software, visando aprimorar o PDSOP.

A análise das codificações proporcionou conhecimentos valiosos, e as representações das limitações, recomendações e sugestões dos especialistas foram avaliadas utilizando as questões do *Technology Acceptance Model (TAM 3)* (MARANGUNIĆ; GRANIĆ, 2015; VENKATESH; BALA, 2008), o que permitiu uma compreensão mais abrangente da aceitação e utilização desses artefatos. Essa

abordagem integrada ofereceu uma visão holística, combinando aspectos quantitativos e qualitativos da avaliação.

As respostas obtidas dos especialistas desempenharam um papel fundamental na evolução do processo. Além disso, a avaliação permitiu identificar áreas específicas para direcionar esforços futuros, visando refinar novas versões do processo, papel e artefatos. Essa melhoria direcionada terá um impacto direto na aceitação e utilização desses artefatos pelas indústrias de desenvolvimento de software.

CAPÍTULO 8 - CONCLUSÃO

Este capítulo apresenta as considerações finais relacionadas à esta pesquisa. A Seção 8.1 descreve a relevância do estudo. A Seção 8.2 aborda as contribuições da pesquisa. A Seção 8.3 exibe as limitações da pesquisa. Por fim, a Seção 8.4 apresenta os trabalhos futuros.

8.1 Relevância da Pesquisa

Para estar em conformidade com a legislação vigente e garantir que os softwares sejam construídos considerando os requisitos de proteção de dados, que decorrem do direito à privacidade, desde as etapas iniciais do processo de desenvolvimento de software, se faz necessário utilizar a abordagem *Privacy by Design (PbD)*. Porém, aplicar os conceitos do PbD em atividades práticas da Engenharia de Software não é uma tarefa trivial devido ao alto nível de abstração de seus princípios, conforme apontado nos estudos primários obtidos a partir da Revisão Sistemática da Literatura e comprovado com o estudo de caso com organizações de desenvolvimento de software.

Na tentativa de preencher esta lacuna alguns estudos fornecem processos de software que apoiam atividades de engenheira de requisitos. Outras pesquisas propõem abordagens limitadas ao modelo tradicional de desenvolvimento, envolvendo fases bem definidas, como análise, design, codificação e testes, as quais dificultam a sua aplicação no contexto ágil de desenvolvimento. Além disso, as pesquisas não mencionam como os princípios do PbD são implementados como atividades práticas em um processo de software, se limitando na identificação de ameaças e vulnerabilidades de privacidade e proteção de dados pessoais. Sendo assim, é importante compreender como os princípios fundamentais do PbD podem ser traduzidos em atividades práticas da Engenharia de Software e inseridos nos diversos processos de desenvolvimento utilizados pelas organizações.

A relevância desta pesquisa está em disponibilizar um processo de desenvolvimento de software que integre os 7 (sete) princípios fundamentais do PbD

às práticas da Engenharia de Software, colocando a proteção de dados pessoais como requisito fundamental, desde as etapas iniciais de desenvolvimento de software. Com isso, os profissionais da área terão apoio para estar em conformidade com as novas legislações e normas em vigor em diversos países.

8.2 Contribuições da Pesquisa

Diversos estudos destacam a importância de abordar os princípios fundamentais do PbD no desenvolvimento de software para salvaguardar a privacidade de dados do titular em todo o ciclo de vida do software. Neste contexto, a pesquisa apresentada neste trabalho segue essa orientação e respalda as seguintes contribuições:

- Cenário de como os princípios do PbD estão sendo aplicados no contexto da Engenharia de Software: Por meio de uma Revisão Sistemática da Literatura destacou-se como a privacidade pode afetar diretamente a qualidade do produto de software e contribui na conscientização sobre a importância de considerar a privacidade e proteção de dados desde as etapas iniciais do processo de desenvolvimento. Além disso, a pesquisa identificou lacunas significativas na aplicação dos princípios do PbD na Engenharia de Software, como carência de modelos, processos e ferramentas específicas para incorporar os princípios ao longo do ciclo de vida do desenvolvimento de software, que podem ser objetivos de pesquisas futuras para a comunidade acadêmica;
- Mapeamento das práticas organizacionais no contexto da privacidade e proteção de dados pessoais: O estudo de caso múltiplo identificou lacunas significativas entre as práticas atuais das organizações e as recomendações legais sobre privacidade de dados pessoais, destacando os desafios enfrentados que influenciam na integração da privacidade aos processos de desenvolvimento de software das organizações, além de fornecer orientações e futuras pesquisas que visam mitigar questões relacionadas à privacidade do usuário no processo de desenvolvimento de software das organizações;

- Mapeamento entre Padrões de Privacidade e Princípios Fundamentais do PbD: O mapeamento realizado poderá auxiliar profissionais de organizações de desenvolvimento de software na tomada de decisão e implementação de soluções adequadas para problemas de privacidade considerando os princípios do PbD;
- Repositório de Instâncias de Padrões de Privacidade: os Padrões de Privacidade possuem uma documentação teórica, extensa e de difícil compreensão. O repositório criado visa auxiliar os profissionais de desenvolvimento de software a compreender os padrões de privacidade por meio de exemplos concretos de aplicação em problemas semelhantes aos enfrentados no dia a dia de um time de desenvolvimento de software;
- Processo de Desenvolvimento de Software Orientado à Privacidade (PDSOP): a principal contribuição desta pesquisa foi a criação do processo capaz de integrar os requisitos de privacidade de dados pessoais desde as etapas iniciais de desenvolvimento de software a fim de preencher a lacuna entre os princípios do PbD e sua aplicação prática no ciclo de vida do desenvolvimento de software. O processo fornece definições de atividades, papel, tarefas e artefatos que auxiliam times de desenvolvimento de software na implementação de privacidade de dados pessoais;
- Repositório PDSOP: O repositório fornece um local centralizado onde os profissionais da indústria de desenvolvimento de software podem acessar todos os materiais relacionados ao PDSOP. A principal contribuição da disponibilização do repositório de modo online é permitir que um número maior de profissionais na indústria de desenvolvimento de software, como desenvolvedores, engenheiros de software, gerentes de projeto e outros profissionais, terão a oportunidade de usufruir os recursos disponíveis para melhorar seus processos de desenvolvimento de software com foco em privacidade e proteção de dados pessoais. Isso amplifica o impacto da pesquisa e promove uma adoção mais ampla dos princípios do PbD na comunidade de desenvolvimento de software.

8.3 Limitações da Pesquisa

As principais limitações identificadas nesta pesquisa são:

- Aplicação prática do PDSOP: o modelo proposto foi avaliado por especialistas com experiência em proteção de dados pessoais e desenvolvimento de software, porém, apesar dos resultados serem positivos, o processo não foi utilizado na prática pela indústria de software;
- Avaliação: como a Lei Geral de Proteção de Dados Pessoais (LGPD) é recente, muitas organizações ainda estão se adaptando à nova realidade e não possuem equipes e profissionais especializados em proteção de dados, com isso, o número de especialistas para realizar a avaliação foi limitado.

8.4 Trabalhos Futuros

Com base na pesquisa realizada, identificam-se as seguintes perspectivas de trabalhos futuros:

- Adaptar o artefato de saída, denominado História de Usuário, para que compreenda requisitos específicos relacionados à proteção de dados pessoais necessários para estar em conformidade com leis/regulamentos específicos. Neste caso, um estudo adicional sobre a legislação pretendida deve ser realizado com o propósito de identificar a obrigatoriedade de determinadas informações que devem ser inseridas como campos obrigatórios no artefato;
- Aplicar o PDSOP em organizações com o intuito de avaliá-lo na prática;
- Realizar estudos de caso com organizações de grande porte a fim de adaptar o PDSOP à modelos de governança de alto nível, como o SAFe *(Scaled Agile Framework)*;
- Implementar um *plugin* para integrar o PDSOP em softwares utilizados pelas organizações para gerenciamento de projetos, como por exemplo, DevOps, Jira, Trello, entre outros.

REFERÊNCIAS BIBLIOGRÁFICAS

(AHMADIAN; STRÜBER; JÜRJENS, 2019) AHMADIAN, A. S.; STRÜBER, D.; JÜRJENS, J. Privacy-enhanced system design modeling based on privacy features. In: **Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing**. p. 1492-1499, 2019.

(AL-MOMANI *et al.*, 2019) AL-MOMANI, A.; KARGL, F.; SCHMIDT, R.; KUNG, A.; BÖSCH, C. A Privacy-Aware V-Model for Software Development. In **2019 IEEE Security and Privacy Workshops (SPW)**, 2019.

(ALHARBI; ZYNGIER; HODKINSON, 2012) ALHARBI, I.; ZYNGIER, S.; HODKINSON, C. An evaluation of the interaction between companies' privacy practices and user information privacy concerns in the success of electronic commerce. In: **European, Mediterranean and Middle Eastern Conference on Information Systems**, 2012.

(ALI; JUTLA; BODORIK, 2016) ALI, N.; JUTLA, D.; BODORIK, P. PIP: An injection pattern for inserting privacy patterns and services in software. In: **Annual Privacy Forum**. Springer, Cham, p. 144-157, 2016.

(ALJOHANI *et al.*, 2016) ALJOHANI, M.; HAWKEY, K.; BLUSTEIN, J. Proposed privacy patterns for privacy preserving healthcare systems in accord with nova scotia's personal health information act. In: **International Conference on Human Aspects of Information Security, Privacy, and Trust**. Springer, Cham, p. 91-102, 2016.

(ALSHAMMARI, 2019) ALSHAMMARI, M. **A principled approach for engineering privacy by design**. 2019. p. 290. Tese de Doutorado - University of Oxford, 2019.

(ALSHAMMARI; SIMPSON, 2017a) ALSHAMMARI, M.; SIMPSON, A. Towards a principled approach for engineering privacy by design. In: **Annual Privacy Forum**. Springer, Cham, p. 161-177, 2017a.

(ALSHAMMARI; SIMPSON, 2017b) ALSHAMMARI, M.; SIMPSON, A. A UML profile for privacy-aware data lifecycle models. In: **Computer Security**. Springer, Cham, p. 189-209, 2017b.

(ALSHAMMARI; SIMPSON, 2017c) ALSHAMMARI, M.; SIMPSON, A. Personal data management: an abstract personal data lifecycle model. In: **International Conference on Business Process Management**. Springer, Cham, p. 685-697, 2017c.

(ALSHAMMARI; SIMPSON, 2018) ALSHAMMARI, M.; SIMPSON, A. Privacy architectural strategies: an approach for achieving various levels of privacy protection. In: **Proceedings of the 2018 Workshop on Privacy in the Electronic Society**. p. 143-154, 2018.

(ALTMAN, 1975) ALTMAN, I. **The environment and social behavior: privacy, personal space, territory, and crowding.** 1975.

(AMANKONA *et al.*, 2021) AMANKONA, V.; ASANTE, A.; OPOKU, M.; OHEMENG-GYAASE, P.; SREKUMAH, C.; PEPRAH, A. K.; AMANKWA-DANQUAH, P. Integrating Privacy-By-Design in e-Health. In: **2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)**. IEEE, p. 1-7, 2021.

(AMNA; POELS, 2022) AMNA, A. R.; POELS, G. Systematic literature mapping of user story research. **IEEE Access**, v. 10, p. 51723-51746, 2022.

(ANDERSON, 2010) ANDERSON, D. J. **Kanban: successful evolutionary change for your technology business**. Blue Hole Press, 2010.

(ANDERSON; CARMICHAEL, 2016) ANDERSON, D. J.; CARMICHAEL, A. **Essential kanban condensed**. Seattle: Lean Kanban University Press, 2016.

(ANDRADE *et al.*, 2022) ANDRADE, V. C.; GOMES, R. D.; REINEHR, S.; FREITAS, C. O. de A.; MALUCELLI, A. Privacy by Design and Software Engineering: a Systematic Literature Review. In: **Proceedings of the XXI Brazilian Symposium on Software Quality**. p. 170-179, 2022.

(ANDRADE *et al.*, 2023) ANDRADE, V. C.; REINEHR, S.; FREITAS, C. O. de A.; MALUCELLI, A. Personal Data Privacy in Software Development Processes: A Practitioner's Point of View. In: **22nd International Conference on Computer and Information Technology (CIT-2023)**. p. 1-8, 2023.

(ANDRADE et al., 2024) ANDRADE, V. C.; RIBEIRO, R. D.; CANTERI, R. dos P.; REINEHR, S.; FREITAS, C. O. de A.; MALUCELLI, A. Privacy in Practice: Exploring Concrete Relationships Between Privacy Patterns and Privacy by Design Principles in Software Engineering. In. **XXVII Ibero-American Conference on Software Engineering (CIbSE 2024)**. p. 1-15, 2024.

(ARAÚJO *et al.*, 2021) ARAÚJO, E.; VILELA, J.; SILVA, C.; ALVES, C. Are my business process models compliant with LGPD? the LGPD4BP method to evaluate and to model LGPD aware business processes. In: **XVII Brazilian Symposium on Information Systems.** p. 1-9, 2021.

(AYALON; TOCH, 2021) AYALON, O.; TOCH, E. User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes. **International Journal of Human-Computer Studies**, p. 102641, 2021.

(BAHILL; GISSING, 1998) BAHILL, A. T.; GISSING, B. Re-evaluating systems engineering concepts using systems thinking. **IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)**, v. 28, n. 4, p. 516-527, 1998.

(BALDASSARRE *et al.*, 2019) BALDASSARRE, M. T.; SANTA BARLETTA, V.; CAIVANO, D.; SCALERA, M. Privacy oriented software development. In: **International Conference on the Quality of Information and Communications Technology**. Springer, Cham, p. 18-32, 2019.

(BALDASSARRE *et al.*, 2020) BALDASSARRE, M. T.; SANTA BARLETTA, V.; CAIVANO, D.; SCALERA, M. Integrating security and privacy in software development. **Software Quality Journal**, v. 28, n. 3, p. 987-1018, 2020.

(BALDASSARRE *et al.*, 2021) BALDASSARRE, M. T.; SANTA BARLETTA, V.; CAIVANO, D.; PICCINNO, A. Integrating Security and Privacy in HCD-Scrum. In: **CHItaly 2021: 14th Biannual Conference of the Italian SIGCHI Chapter**. p. 1-5, 2021.

(BARGH; CHOENNI, 2019) BARGH, M. S.; CHOENNI, S. Towards Applying Design-Thinking for Designing Privacy-Protecting Information Systems. In: **2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)**. IEEE, p. 196-202, 2019.

(BECK, 2000) BECK, K. **Extreme programming explained: embrace change**. addison-wesley professional, 2000.

(BEN-SASSON; GREENBERG, 2023) BEN-SASSON, H.; GREENBERG, R. **38TB of data accidentally exposed by Microsoft AI researchers.** Disponível em: <https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers>. Acesso em: 24 abr. 2024.

(BIER *et al.*, 2012) BIER, C.; BIRNSTILL, P.; KREMPEL, E.; VAGTS, H.; BEYERER, J. Enhancing privacy by design from a developer's perspective. In: **Annual Privacy Forum**. Springer, Berlin, Heidelberg, p. 73-85, 2012.

(BLIX; ELSHEKEIL; LAOYOOKHONG, 2017) BLIX, F.; ELSHEKEIL, S. A.; LAOYOOKHONG, S. Data protection by design in systems development: From legal requirements to technical solutions. In: **2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)**. IEEE, p. 98-103, 2017.

(BORITZ; WON; SUNDARRAJ, 2008) BORITZ, J. E.; NO, W. G.; SUNDARRAJ, R. P. Internet privacy in e-commerce: Framework, review, and opportunities for future research. In: **Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)**. IEEE, p. 1-10, 2008

(BOURQUE; FAIRLEY, 2014) BOURQUE, P.; FAIRLEY, R. E. Guide to the Software Engineering Body of Knowledge (SWEBoK(r)): Version 3.0. **IEEE software**, v. 3, p. 348, 2014.

(BOZDAG, 2020) BOZDAG, E. **Privacy at Speed: Privacy by Design at Uber**. Disponível em: <https://www.usenix.org/conference/enigma2020/presentation/bozdag>. Acesso em: 09 ago. 2021.

(BRASIL, 1966) BRASIL. **Lei nº 5.172, de 25 de Outubro de 1966**. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm>. Acesso em: 9 out. 2023.

(BRASIL, 2018a) BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27 dez. 2023.

(BRASIL, 2018b) BRASIL. **Lei nº 13.787, de 27 de Dezembro de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm#:~:text=6o>. Acesso em: 27 dez. 2023.

(BROWNING, 2021) BROWNING, K. **A “potentially disastrous” data breach hits Twitch, the livestreaming site**. Disponível em: <https://www.nytimes.com/2021/10/06/technology/twitch-data-breach.html>. Acesso em: 7 jun. 2023.

(BU *et al.*, 2020) BU, F.; WANG, N.; JIANG, B.; LIANG, H. “Privacy by Design” implementation: Information system engineers’ perspective. **International Journal of Information Management**, v. 53, p. 102124, 2020.

(BU *et al.*, 2021) BU, F.; WANG, N.; JIANG, B.; JIANG, Q. Motivating information system engineers’ acceptance of Privacy by Design in China: An extended UTAUT model. **International Journal of Information Management**, v. 60, p. 102358, 2021.

(BUGEJA; JACOBSSON, 2020) BUGEJA, J.; JACOBSSON, A. On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces. In: **14th IFIP International Summer School on Privacy and Identity Management (Privacy and Identity)**. p. 126-141, 2020.

(CADWALLADR; GRAHAM-HARRISON, 2018) CADWALLADR, C.; GRAHAM-HARRISON, E. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 10 mar. 2021.

(CAIZA *et al.*, 2017) CAIZA, J. C.; MARTÍN, Y. S.; DEL ALAMO, J. M.; GUAMÁN, D. S. Organizing design patterns for privacy: a taxonomy of types of relationships. In: **Proceedings of the 22nd European Conference on Pattern Languages of Programs**. p. 1-11, 2017.

(CAVOUKIAN, 2009a) CAVOUKIAN, A. Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices. **Information and Privacy Commissioner of Ontario, Canada**, v. 5, p. 40, 2009a.

(CAVOUKIAN, 2009b) CAVOUKIAN, A. **Privacy by design... take the challenge.** 2009b.

(CAVOUKIAN, 2012a) CAVOUKIAN, A. Operationalizing Privacy by Design: A Guide to Implementing. **Commun ACM**, v. 55, n. 9, p. 7, 2012a.

(CAVOUKIAN, 2012b) CAVOUKIAN, A. Privacy by design [leading edge]. **IEEE Technology and Society Magazine**, v. 31, n. 4, p. 18-19, 2012b.

(CAVOUKIAN; SHAPIRO; CRONK, 2014) CAVOUKIAN, A.; SHAPIRO, S.; CRONK, R. J. **Privacy engineering: Proactively embedding privacy, by design**. Office of the Information and Privacy Commissioner, 2014.

(CHANDER; LAND, 2014) CHANDER, A.; LAND, M. United Nations General Assembly Resolution on the Right to Privacy in the Digital Age. **International Legal Materials**, v. 53, n. 4, p. 727-731, 2014.

(CHANDRAMOULI; ARGUEDAS; IZQUIERDO, 2013) CHANDRAMOULI, K.; ARGUEDAS, V. F.; IZQUIERDO, E. Knowledge modeling for privacy-by-design in smart surveillance solution. In: **10th IEEE International Conference on Advanced Video and Signal Based Surveillance**. IEEE, 2013. p. 171-176, 2013.

(CHARMAZ, 2006) CHARMAZ, K. **Constructing grounded theory: A practical guide through qualitative analysis.** sage, 2006.

(CHEN; WILLIAMS, 2013) CHEN, S.; WILLIAMS, M. Grounding Privacy-by-Design for information systems. In: **Pacific Asia Conference on Information Systems**. Association of Information Systems, p. 107, 2013

(CHOMA; ZAINA; BERALDO, 2016) CHOMA, J.; ZAINA, L.; BERALDO, D. UserX story: Incorporating UX aspects into user stories elaboration. In: **Human-Computer Interaction. Theory, Design, Development and Practice: 18th International Conference, HCI International 2016, Toronto, ON, Canada, July 17-22, 2016. Proceedings, Part I 18**. Springer International Publishing, p. 131-140, 2016.

(CHUNG *et al.*, 2004) CHUNG, E. S.; HONG, J. I.; LIN, J.; PRABAKER, M. K.; LANDAY, J. A.; LIU, A. L. Development and evaluation of emerging design patterns for ubiquitous computing. In: **Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques**. p. 233-242, 2004.

(COHN, 2004) COHN, M. **User Stories Applied: For agile software development.** Addison-Wesley Professional, 2004.

(COLESKY *et al.*, 2018) COLESKY, M.; CAIZA, J. C.; DEL ALAMO, J. M.; HOEPMAN, J. H.; MARTÍN, Y. S. A system of privacy patterns for user control. In: **Proceedings of the 33rd Annual ACM Symposium on Applied Computing**. p. 1150-1156, 2018.

(COLESKY; GHANAVATI, 2016) COLESKY, M.; GHANAVATI, S. Privacy shielding by design - a strategies case for near-compliance. In: **2016 24th International Requirements Engineering Conference Workshops (REW)**. IEEE, p. 271-275, 2016.

(COLESKY; HOEPMAN; HILLEN, 2016) COLESKY, M.; HOEPMAN, J.; HILLEN, C. A critical analysis of privacy design strategies. In: **2016 IEEE Security and Privacy Workshops (SPW)**. IEEE, p. 33-40, 2016.

(COLLIS; HUSSEY, 2009) COLLIS, J.; HUSSEY, R. **Business research: A practical guide for undergraduate and postgraduate students.** Palgrave MacMillan, UK, 2009.

(CUNNINGHAM, 2001) CUNNINGHAM, W. **Manifesto for Agile Software Development**. Disponível em: <https://agilemanifesto.org>. Acesso em: 27 mar. 2021.

(CURCIO *et al.*, 2018) CURCIO, K.; NAVARRO, T.; MALUCELLI, A.; REINEHR, S. Requirements engineering: A systematic mapping study in agile software development. **Journal of Systems and Software**, v. 139, p. 32-50, 2018.

(DANEZIS *et al.*, 2015) DANEZIS, G.; DOMINGO-FERRER, J.; HANSEN, M.; HOEPMAN, J. H.; METAYER, D. L.; TIRTEA, R.; SCHIFFNER, S. Privacy and data

protection by design-from policy to engineering. **arXiv preprint arXiv:1501.03726**, 2015.

(DEGELING *et al.*, 2016) DEGELING, M.; LENTZSCH, C.; NOLTE, A.; HERRMANN, T.; LOSER, K. U. Privacy by socio-technical design: A collaborative approach for privacy friendly system design. In: **2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)**. IEEE, p. 502-505, 2016.

(DEGELING; LOSER, 2013) DEGELING, M.; LOSER, K. An Approach to introduce Privacy by Design in Agile App-Development. **PRIVACY AND EMERGING SCIENCES AND TECHNOLOGIES**, p. 17, 2013.

(DELEERSNYDER, 2018) DELEERSNYDER, S. **Adding Privacy by Design in Secure Application Development**. Disponível em: <https://owasp.org/www-pdf-archive/TOREON_Adding_Privacy_by_Design_in_Secure_Application_Development_v20180412.pdf>. Acesso em: 9 ago. 2021.

(DELLA MEA, 2001) DELLA MEA, V. What is e-Health (2): The death of telemedicine?. **Journal of medical Internet research**, v. 3, n. 2, p. e834, 2001.

(DENG *et al.*, 2011) DENG, M.; WUYTS, K.; SCANDARIATO, R.; PRENEEL, B.; JOOSEN, W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. **Requirements Engineering**, v. 16, n. 1, p. 3-32, 2011.

(DENNEHY; CONBOY, 2017) DENNEHY, D.; CONBOY, K. Going with the flow: An activity theory analysis of flow techniques in software development. **Journal of Systems and Software**, v. 133, p. 160-173, 2017.

(DIJKSTRA, 1972) DIJKSTRA, E. W. The humble programmer. **Communications of the ACM**, v. 15, n. 10, p. 859-866, 1972.

(DODERO *et al.*, 2019) DODERO, J. M.; RODRIGUEZ-GARCIA, M.; RUIZ-RUBE, I.; PALOMO-DUARTE, M. Privacy-preserving reengineering of model-view-controller application architectures using linked data. **Journal of Web Engineering**, v. 18, n. 7, p. 695-728, 2019.

(DRIEL, 2016) DRIEL, R. VAN. **Agile Scrum and the GDPR**. Disponível em: <https://www.linkedin.com/pulse/agile-scrum-gdpr-ruud-van-driel-cissp/>. Acesso em: 9 ago. 2021.

(ECLIPSE FOUNDATION, 2023) ECLIPSE FOUNDATION. **Desktop IDEs.** Disponível em: <https://www.eclipse.org/ide/>. Acesso em: 5 nov. 2023.

(EU, 2016) EU. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. **Official Journal of the European Union (OJ)**, v. 59, n. 1–88, p. 294, 2016.

(FLEISS; LEVIN; PAIK, 2013) FLEISS, J. L.; LEVIN, B.; PAIK, M. C. **Statistical methods for rates and proportions**. john wiley & sons, 2013.

(FOUKIA; BILLARD; SOLANA, 2016) FOUKIA, N.; BILLARD, D.; SOLANA, E. PISCES: A framework for privacy by design in IoT. In: **2016 14th Annual Conference on Privacy, Security and Trust (PST)**. IEEE, p. 706-713, 2016.

(FREITAS, 2022) FREITAS, C. O. DE A. Riscos e Proteção de Dados Pessoais. **Rede de Direito Digital, Intelectual & Sociedade**, v. 2, n. 4, p. 225–247, 2022.

(GALVEZ; GURSES, 2018) GALVEZ, R.; GURSES, S. The odyssey: Modeling privacy threats in a brave new world. In: **2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)**. IEEE, p. 87-94, 2018.

(GAUDINO, 2011) GAUDINO, F. R. Applied sciences in biomedical and ICT from the perspective of the patient's right to data privacy and security: turning a zero-sum into a positive-sum game. In: **Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies**. p. 1-6, 2011.

(GILL; HENDERSON-SELLERS; NIAZI, 2018) GILL, A. Q.; HENDERSON-SELLERS, B.; NIAZI, M. Scaling for agility: A reference model for hybrid traditional-agile software development methodologies. **Information Systems Frontiers**, v. 20, n. 2, p. 315-341, 2018.

(GRAF *et al.*, 2010) GRAF, C.; WOLKERSTORFER, P.; GEVEN, A.; TSCHELIGI, M. A pattern collection for privacy enhancing technology. In: **The 2nd Int. Conf. on Pervasive Patterns and Applications (PATTERNS 2010)**. p. 21-26, 2010.

(GRALHA *et al.*, 2022) GRALHA, C.; PEREIRA, R.; GOULÃO, M.; ARAUJO, J. Assessing user stories: the influence of template differences and gender-related problem-solving styles. **Requirements Engineering**, v. 27, n. 4, p. 521-544, 2022.

(GUERRIERO *et al.*, 2017) GUERRIERO, M.; TAMBURRI, D. A.; RIDENE, Y.; MARCONI, F.; BERSANI, M. M.; ARTAC, M. Towards DevOps for Privacy-by-Design in Data-Intensive Applications: A Research Roadmap. In: **Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion**. p. 139-144, 2017.

(GUJARATI; PORTER, 2010) GUJARATI, D.; PORTER, D. **Essentials of econometrics.** Sage Publications, 2010.

(GURSES; DEL ALAMO, 2016) GÜRSES, S.; DEL ALAMO, J. M. Privacy engineering: Shaping an emerging field of research and practice. **IEEE Security & Privacy**, v. 14, n. 2, p. 40-46, 2016.

(GÜRSES; TRONCOSO; DIAZ, 2011) GÜRSES, S.; TRONCOSO, C.; DIAZ, C. Engineering privacy by design. **Computers, Privacy & Data Protection**, v. 14, n. 3, p. 25, 2011.

(GÜRSES; TRONCOSO; DIAZ, 2015) GÜRSES, S.; TRONCOSO, C.; DIAZ, C. Engineering privacy by design reloaded. In: **Amsterdam Privacy Conference**. p. 1-21, 2015.

(HADAR *et al.*, 2018) HADAR, I.; HASSON, T.; AYALON, O.; TOCH, E.; BIRNHACK, M.; SHERMAN, S.; BALISSA, A. Privacy by designers: software developers' privacy mindset. **Empirical Software Engineering**, v. 23, n. 1, p. 259-289, 2018.

(HAFIZ, 2006) HAFIZ, M. A collection of privacy design patterns. In: **Proceedings of the 2006 conference on Pattern languages of programs**. p. 1-13, 2006.

(HATAMIAN, 2020) HATAMIAN, M. Engineering privacy in smartphone apps: A technical guideline catalog for app developers. **IEEE Access**, v. 8, p. 35429-35445, 2020.

(HAZEYAMA *et al.*, 2016) HAZEYAMA, A.; WASHIZAKI, H.; YOSHIOKA, N.; KAIYA, H.; OKUBO, T. Literature survey on technologies for developing privacy-aware software. In: **2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)**. IEEE, p. 86-91, 2016.

(HOEL; GRIFFITHS; CHEN, 2017) HOEL, T.; GRIFFITHS, D.; CHEN, W. The influence of data protection and privacy frameworks on the design of learning analytics systems. In: **Proceedings of the seventh international learning analytics & knowledge conference**. p. 243-252, 2017.

(HOEPMAN, 2014) HOEPMAN, J. Privacy design strategies. In: **IFIP International Information Security Conference**. Springer, Berlin, Heidelberg, p. 446-459, 2014.

(HÖRBE; HÖTZENDORFER, 2015) HÖRBE, R.; HÖTZENDORFER, W. Privacy by design in federated identity management. In: **2015 IEEE Security and Privacy Workshops**. IEEE, p. 167-174, 2015.

(HUANG; KUSIAK, 1996) HUANG, C.; KUSIAK, A. Overview of Kanban systems. **Computer Integrated Manufacturing**, v. 9, n. 3, p. 169--189, 1996.

(INFOMONEY, 2022) INFOMONEY. **Tudo sobre Pix: entenda como funciona o sistema de pagamentos do Banco Central.** Disponível em: <https://www.infomoney.com.br/guias/pix/>. Acesso em: 22 dez. 2023.

(INFOMONEY, 2023) INFOMONEY. **Deezer sofre vazamento de dados que expõe 220 milhões de usuários**. Disponível em: <https://www.infomoney.com.br/negocios/deezer-sofre-vazamento-de-dados-que-expoe-220-milhoes-de-usuarios/>. Acesso em: 22 dez. 2023.

(ISO/IEC 27701, 2019) ISO/IEC 27701. **Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines.** International Organization for Standardization, 2019.

(ISO/IEC 29100, 2011) ISO/IEC 29100. **Information technology - Security techniques - Privacy framework**. International Organization for Standardization, 2011.

(JUTLA; BODORIK; ALI, 2013) JUTLA, D. N.; BODORIK, P.; ALI, S. Engineering privacy for big data apps with the unified modeling language. In: **2013 IEEE International Congress on Big Data**. IEEE, p. 38-45, 2013.

(KALLONIATIS; KAVAKLI; GRITZALIS, 2008) KALLONIATIS, C.; KAVAKLI, E.; GRITZALIS, S. Addressing privacy requirements in system design: the PriS method. **Requirements Engineering**, v. 13, n. 3, p. 241-255, 2008.

(KANNAN *et al.*, 2019) KANNAN, V.; BASIT, M. A.; BAJAJ, P.; CARRINGTON, A. R.; DONAHUE, I. B.; FLAHAVEN, E. L.; TOOMAY, S. M. User stories as lightweight requirements for agile clinical decision support development. **Journal of the American Medical Informatics Association**, v. 26, n. 11, p. 1344-1354, 2019.

(KIMURA; TERADA, 1981) KIMURA, O.; TERADA, H. Desiǵn and analysis of Pull System, a method of multi-staǵe production control. **The International Journal Of Production Research**, v. 19, n. 3, p. 241-253, 1981.

(KISSEL *et al.*, 2008) KISSEL, R.; STINE, K.; SCHOLL, M.; ROSSMAN, H.; FAHLSING, J.; GULICK, J. **Security Considerations in the System Development Life Cycle.** NIST Special Publication 800-64 Revision 2. Gaithersburg: 2008.

(KITCHENHAM; CHARTERS, 2007) KITCHENHAM, B.; CHARTERS, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. **EBSE Technical Report - EBSE-2007-01**, p. 1-57, 2007.

(KOLKOWSKA, 2015) KOLKOWSKA, E. Privacy principles in design of smart homes systems in elderly care. In: **International Conference on Human Aspects of Information Security, Privacy, and Trust**. Springer, Cham, p. 526-537, 2015.

(KOO; LI, 2016) KOO, T.; LI, M. A guideline of selecting and reporting intraclass correlation coefficients for reliability research. **Journal of chiropractic medicine**, v. 15, n. 2, p. 155-163, 2016.

(KOST *et al.*, 2011) KOST, M.; FREYTAG, J. C.; KARGL, F.; KUNG, A. Privacy verification using ontologies. In: **2011 Sixth International Conference on Availability, Reliability and Security**. IEEE, p. 627-632, 2011.

(KUNG, 2014) KUNG, A. PEARs: privacy enhancing architectures. In: **Annual Privacy Forum**. Springer, Cham, p. 18-29, 2014.

(KUNG; FREYTAG; KARGL, 2011) KUNG, A; FREYTAG, J.; KARGL, F. Privacy-by-design in its applications. In: **2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks**. IEEE, p. 1-6, 2011.

(KUNG; JOUVRAY; COUDERT, 2015) KUNG, A.; JOUVRAY, C.; COUDERT, F.. SALT frameworks to tackle surveillance and privacy concerns. In: **2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)**. IEEE, p. 665-673, 2015.

(LANDIS; KOCH, 1977) LANDIS, J.; KOCH, G. The measurement of observer agreement for categorical data. **Biometrics**, p. 159-174, 1977.

(LE MÉTAYER, 2013) LE MÉTAYER, D. Privacy by design: a formal framework for the analysis of architectural choices. In: **Proceedings of the third ACM conference on Data and application security and privacy**. p. 95-104, 2013.

(LENHARD; FRITSCH; HEROLD, 2017) LENHARD, J.; FRITSCH, L.; HEROLD, S. A literature study on privacy patterns research. In: **2017 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)**. IEEE, p. 194-201, 2017.

(LOBATO; FERNANDEZ; ZORZO, 2009) LOBATO, L. L.; FERNANDEZ, E. B.; ZORZO, S. D. Patterns to support the development of privacy policies. In: **2009 International Conference on Availability, Reliability and Security**. IEEE, p. 744-749, 2009.

(LUCASSEN; B; WERF, 2016) LUCASSEN, G.; DALPIAZ, F.; WERF, J. M. E. V. D.; BRINKKEMPER, S. The use and effectiveness of user stories in practice. In: **Requirements Engineering: Foundation for Software Quality: 22nd International Working Conference, REFSQ 2016, Gothenburg, Sweden, March 14-17, 2016, Proceedings 22**. Springer International Publishing, p. 205-222, 2016.

(MALAR, 2022) MALAR, J. **Banco Central anuncia vazamento de dados ligados a mais de 130 mil chaves Pix.** Disponível em: <https://www.cnnbrasil.com.br/economia/banco-central-anuncia-vazamento-de-dados-ligados-a-mais-de-130-mil-chaves-pix/>. Acesso em: 11 abr. 2023.

(MARANGUNIĆ; GRANIĆ, 2015) MARANGUNIĆ, N.; GRANIĆ, A. Technology acceptance model: a literature review from 1986 to 2013. **Universal access in the information society**, v. 14, n. 1, p. 81-95, 2015.

(MARTÍN *et al.*, 2014) MARTÍN, Y.; DEL ALAMO, J. M.; YELMO, J. C. Engineering privacy requirements valuable lessons from another realm. In: **2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)**. IEEE, p. 19-24, 2014.

(MIRZA; DATTA, 2019) MIRZA, M. S.; DATTA, S. Strengths and Weakness of Traditional and Agile Processes-A Systematic Review. **J. Softw.**, v. 14, n. 5, p. 209-219, 2019.

(MORAL-GARCÍA *et al.*, 2011) MORAL-GARCÍA, S.; ORTIZ, R.; MORAL-RUBIO, S.; GARZÁS, J.; FERNÁNDEZ-MEDINA, E. A New Pattern Template to Support the Design of Security Architectures: A Case Study. **International Journal on Advances in Security.** v. 4, n. 3 & 4, 2011.

(MORALES-TRUJILLO *et al.*, 2019) MORALES-TRUJILLO, M. E.; GARCÍA-MIRELES, G. A.; MATLA-CRUZ, E. O.; PIATTINI, M. A Systematic Mapping Study of Privacy by Design in Software Engineering. **CLEI Electronic Journal**, v. 22, n. 1, 2019.

(MORALES-TRUJILLO; GARCIA-MIRELES, 2018) MORALES-TRUJILLO, M. E.; GARCIA-MIRELES, G. A. Extending ISO/IEC 29110 basic profile with privacy-by-design approach: A case study in the health care sector. In: **2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)**. IEEE, p. 56-64, 2018.

(MORTON; SASSE, 2012) MORTON, A.; SASSE, M. A. Privacy is a process, not a PET: a theory for effective privacy practice. In: **Proceedings of the 2012 New Security Paradigms Workshop**. p. 87-104, 2012.

(NOTARIO *et al.*, 2014) NOTARIO, N.; CRESPO, A.; KUNG, A.; KROENER, I.; LE MÉTAYER, D.; TRONCOSO, C.; MARTÍN, Y. S. Pripare: a new vision on engineering privacy and security by design. In: **Cyber Security and Privacy Forum**. Springer, Cham, p. 65-76, 2014.

(NOTARIO *et al.*, 2015) NOTARIO, N.; CRESPO, A.; MARTÍN, Y. S.; DEL ALAMO, J. M.; LE MÉTAYER, D.; ANTIGNAC, T.; WRIGHT, D. PRIPARE: integrating privacy best practices into a privacy engineering methodology. In: **2015 IEEE Security and Privacy Workshops**. IEEE, p. 151-158, 2015.

(OETZEL; SPIEKERMANN, 2012) OETZEL, M. C.; SPIEKERMANN, S. Privacy-by-design through systematic privacy impact assessment: a design science approach. **European Journal of Information Systems (EJIS).** 2012.

(PEDROZA *et al.*, 2021) PEDROZA, G.; MUNTES-MULERO, V.; MARTIN, Y. S.; MOCKLY, G. A Model-based approach to realize privacy and data protection by design. In: **2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)**. IEEE, p. 332-339, 2021.

(PEFFERS *et al.*, 2007) PEFFERS, K.; TUUNANEN, T.; ROTHENBERGER, M. A.; CHATTERJEE, S. A design science research methodology for information systems research. **Journal of management information systems**, v. 24, n. 3, p. 45-77, 2007.

(PEIXOTO *et al.*, 2023) PEIXOTO, M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C.; VILELA, J.; ARAÚJO, J.; GORSCHEK, T. The perspective of Brazilian software developers on data privacy. **Journal of Systems and Software**, v. 195, p. 111523, 2023.

(PEIXOTO, 2020) PEIXOTO, M. M. Privacy Requirements Engineering in Agile Software Development: a Specification Method. In: **REFSQ Workshops**. 2020.

(PEIXOTO, 2021) PEIXOTO, M. M. **A privacy requirements specification method for Agile Software Development based on exploratory studies.** 2021. p. 314. Tese de Doutorado - Universidade Federal de Pernambuco, Recife, 2021.

(PERERA *et al.*, 2016) PERERA, C.; MCCORMICK, C.; BANDARA, A. K.; PRICE, B. A.; NUSEIBEH, B. Privacy-by-design framework for assessing internet of things applications and platforms. In: **Proceedings of the 6th International Conference on the Internet of Things**. p. 83-92, 2016.

(PERERA *et al.*, 2020) PERERA, C.; BARHAMGI, M.; BANDARA, A. K.; AJMAL, M.; PRICE, B.; NUSEIBEH, B. Designing privacy-aware internet of things applications. **Information Sciences**, v. 512, p. 238-257, 2020.

(PETERSEN; VAKKALANKA; KUZNIARZ, 2015) PETERSEN, K.; VAKKALANKA, S.; KUZNIARZ, L. Guidelines for conducting systematic mapping studies in software engineering: An update. **Information and Software Technology**, v. 64, p. 1-18, 2015.

(PETKAUSKAS, 2024) PETKAUSKAS, V. **Mother of all breaches reveals 26 billion records:** what we know so far. Disponível em: <https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/#:~:text=Mother%20of%20all%20breaches%20reveals,what%20we%20know%20so%20far&text=Image%20by%20Cybernews.,mind-boggling%2026%20billion%20records.>. Acesso em: 17 fev. 2024.

(PFITZMANN; HANSEN, 2010) PFITZMANN, A.; HANSEN, M. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. 2010.

(PFLÜGLER; WIESCHE, 2018) PFLÜGLER, C.; WIESCHE, M.; KRCMAR, H. Subgroups in agile and traditional IT project teams. In: **Proceedings of the 51st Hawaii International Conference on System Sciences**. 2018.

(PIRAS *et al.*, 2019) PIRAS, L.; AL-OBEIDALLAH, M. G.; PRAITANO, A.; TSOHOU, A.; MOURATIDIS, H.; CRESPO, B. G. N.; ZORZINO, G. G. DEFeND architecture: a privacy by design platform for GDPR compliance. In: **International Conference on Trust and Privacy in Digital Business**. Springer, Cham, p. 78-93, 2019.

(POPPENDIECK; CUSUMANO, 2012) POPPENDIECK, M.; CUSUMANO, M. A. Lean software development: A tutorial. **IEEE software**, v. 29, n. 5, p. 26-32, 2012.

(POPPENDIECK; POPPENDIECK, 2003) POPPENDIECK, M.; POPPENDIECK, T. **Lean software development: an agile toolkit**. Addison-Wesley, 2003.

(POWER, 2014) POWER, K. Definition of ready: An experience report from teams at cisco. In: **International Conference on Agile Software Development**. Springer, Cham, p. 312-319, 2014.

(POWER; CONBOY, 2015) POWER, K. A Metric-Based Approach to Managing Architecture-Related Impediments in Product Development Flow: an industry case study from Cisco. In: **2015 IEEE/ACM 2nd International Workshop on Software Architecture and Metrics.** IEEE, p. 15-21, 2015.

(PRIES; QUIGLEY, 2010) PRIES, K. H.; QUIGLEY, J. M. **Scrum project management**. CRC press, 2010.

(RAINER; HALL, 2002) RAINER, A.; HALL, T. Key success factors for implementing software process improvement: a maturity-based analysis. **Journal of Systems and Software**, v. 62, n. 2, p. 71-84, 2002.

(REDAÇÃO VEJA, 2018) REDAÇÃO VEJA. **Banco Inter vai pagar R$ 1,5 milhão por vazamento de dados de clientes**. Disponível em: <https://veja.abril.com.br/economia/banco-inter-vai-pagar-r-15-milhao-por-vazamento-de-dados-de-clientes/>. Acesso em: 24 mai. 2021.

(REDDY; KUMAR, 2020) REDDY, K. S. M.; KUMAR, V. V. Necessity of Agile Development Models in Now-a-Day Software Development. **A Journal of Composition Theory**, p. 25-28, 2020.

(RIGHINI; CALDERONI; MAIO, 2022) RIGHINI, S.; CALDERONI, L.; MAIO, D. A privacy-aware zero interaction smart mobility system. **IEEE Access**, v. 10, p. 11924-11937, 2022.

(ROHR, 2021) ROHR, A. **Megavazamentos de dados expõem informações de 223 milhões de números de CPF**. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>. Acesso em: 24 maio. 2021.

(ROMANOSKY *et al.*, 2006) ROMANOSKY, S.; ACQUISTI, A.; HONG, J.; CRANOR, L. F.; FRIEDMAN, B. Privacy patterns for online interactions. In: **Proceedings of the 2006 conference on Pattern languages of programs**. p. 1-9, 2006.

(ROMANOU, 2018) ROMANOU, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. **Computer law & security review**, v. 34, n. 1, p. 99-110, 2018.

(ROSENBERG, 2018) ROSENBERG, M. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. Disponível em: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Acesso em: 10 mar. 2021.

(ROWAN; DEHLINGER, 2014) ROWAN, M.; DEHLINGER, J. Encouraging privacy by design concepts with privacy policy auto-generation in eclipse (page). In: **Proceedings of the 2014 Workshop on Eclipse Technology eXchange**. p. 9-14, 2014.

(ROYCE, 1970) ROYCE, W. W. Managing the development of large software systems: concepts and techniques. In: **Proceedings of the 9th international conference on Software Engineering**. p. 328-338, 1970.

(RYGGE; JØSANG, 2018) RYGGE, H.; JØSANG, A. Threat poker: solving security and privacy threats in agile software development. In: **Nordic Conference on Secure IT Systems**. Springer, Cham, p. 468-483, 2018.

(SAKUL-UNG; SMANCHAT, 2019) SAKUL-UNG, P.; SMANCHAT, S. Towards Privacy Framework in Software Development Projects and Applications: An Integrated Framework. In: **2019 Research, Invention, and Innovation Congress (RI2C)**. IEEE, p. 1-6, 2019.

(SALDAÑA, 2013) SALDAÑA, J. **The coding manual for qualitative researchers**. 2 ed. SAGE Publications Limited, 2013.

(SCHNEIDER, 2018) SCHNEIDER, G. Is privacy by construction possible?. In: **International Symposium on Leveraging Applications of Formal Methods**. Springer, Cham, p. 471-485, 2018.

(SCHWABER; BEEDLE, 2002) SCHWABER, K.; BEEDLE, M. **Agile software development with Scrum**. Upper Saddle River: Prentice Hall, 2002.

(SCHWABER; SUTHERLAND, 2020) SCHWABER, K.; SUTHERLAND, J. O Guia Definitivo para o Scrum: As Regras do Jogo. **Harvard Business Review, Boston**, v. IV, p. 16, 2020.

(SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, 1973) SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS. **Records, computers and the rights of citizens**. RAND Corporation, Santa Monica, CA, Tech. Rep. 1973.

(SEMANTHA; AZAM, 2021) Semantha, F. H.; Azam, S.; Shanmugam, B.; Yeo, K. C.; Beeravolu, A. R. A conceptual framework to ensure privacy in patient record management system. **IEEE Access**, v. 9, p. 165667-165689, 2021.

(SENARATH; ARACHCHILAGE, 2018) SENARATH, A.; ARACHCHILAGE, N. A. G. Why developers cannot embed privacy into software systems? An empirical investigation. In: **Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018**. p. 211-216, 2018.

(SENARATH; ARACHCHILAGE; SLAY, 2017) SENARATH, A.; ARACHCHILAGE, N. AG; SLAY, J. Designing Privacy for You: A Practical Approach for User-Centric Privacy. In: **International Conference on Human Aspects of Information Security, Privacy, and Trust**. Springer, Cham, p. 739-752, 2017.

(SHISHKOV; JANSSEN, 2018) SHISHKOV, B.; JANSSEN, M. Enforcing context-awareness and privacy-by-design in the specification of information systems. In: **International Symposium on Business Modeling and Software Design**. Springer, Cham, p. 87-111, 2018.

(SILJEE, 2015) SILJEE, J. Privacy transparency patterns. In: **Proceedings of the 20th european conference on pattern languages of programs**. p. 1-11, 2015.

(SPHERE IDENTITY, 2018) SPHERE IDENTITY. **GDPR and Privacy by Design: what developers need to know**. Disponível em: <https://medium.com/sphere-identity/gdpr-and-privacy-by-design-what-developers-need-to-know-fa5a936da65a>. Acesso em: 9 ago. 2021.

(SPIEKERMANN, 2012) SPIEKERMANN, S. The challenges of privacy by design. **Communications of the ACM**, v. 55, n. 7, p. 38-40, 2012.

(STAATS, 2023) STAATS, R. **Integrating Privacy by Design into your UI design strategy**. Disponível em: <https://www.secretstache.com/blog/integrating-privacy-by-design/>. Acesso em: 9 ago. 2021.

(STEVOVIC *et al.*, 2015a) STEVOVIC, J.; SOTTOVIA, P.; MARCHESE, M.; ARMELLIN, G. BPM Supported Privacy by Design for Cross-Organization Business Processes. In: **Service-Oriented Computing-ICSOC 2014 Workshops**. Springer, Cham, p. 71-83, 2015a.

(STEVOVIC *et al.*, 2015b) STEVOVIC, J.; BASSI, E.; GIORI, A.; CASATI, F.; ARMELLIN, G. Enabling privacy by design in medical records sharing. In: **Reforming European Data Protection Law**. Springer, Dordrecht, p. 385-406, 2015b.

(STEYAERT, 2017) STEYAERT, P. **Essential Upstream Kanban**. Seatle: University Press, 2017.

(STRAUSS; CORBIN, 1998) STRAUSS, A.; CORBIN, J. **Basics of qualitative research techniques**. 1998.

(SUGIMORI *et al.*, 1977) SUGIMORI, Y.; KUSUNOKI, K.; CHO, F.; UCHIKAWA, S. Toyota production system and kanban system materialization of just-in-time and respect-for-human system. **The international journal of production research**, v. 15, n. 6, p. 553-564, 1977.

(SUPHAKUL; SENIVONGSE, 2017) SUPHAKUL, T.; SENIVONGSE, T. Development of privacy design patterns based on privacy principles and UML. In: **2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)**. IEEE, p. 369-375, 2017.

(TAHAEI; FRIK; VANIEA, 2021) TAHAEI, M.; FRIK, A.; VANIEA, K. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In: **Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems**. p. 1-15, 2021.

(TAKEUCHI; NONAKA, 1986) TAKEUCHI, H.; NONAKA, I. The new new product development game. **Harvard business review**, v. 64, n. 1, p. 137-146, 1986.

(TAMBURRI, 2020) TAMBURRI, D. A. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. **Information Systems**, v. 91, p. 101469, 2020.

(TEAM, 2018) TEAM, C. 4 N. I. **Revealed: Cambridge Analytica data on thousands of Facebook users still not deleted**. Disponível em: <https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted>. Acesso em: 10 mar. 2021.

(THE OPEN GROUP, 2021) THE OPEN GROUP. **The TOGAF® Standard**. Disponível em: <https://www.opengroup.org/togaf>. Aceso em: 4 mai. 2021.

(TIDY; MOLLOY, 2021) TIDY, J.; MOLLOY, D. **Twitch confirms massive data breach.** Disponível em: <https://www.bbc.com/news/technology-58817658>. Acesso em: 7 jun. 2023.

(UC BERKELEY SCHOOL OF INFORMATION, 2024) UC BERKELEY SCHOOL INFORMATION. **Privacy Patterns**. Disponível em: <https://privacypatterns.org/>. Acesso em: 29 mar. 2024.

(VAIDYA; MOUFTAH, 2018) VAIDYA, B.; MOUFTAH, H. T. Protecting the privacy of electricity consumers in the smart city. **Transportation and Power Grid in Smart Cities: Communication Networks and Services**, p. 529-554, 2018.

(VAN REST *et al.*, 2014) VAN REST, J.; BOONSTRA, D.; EVERTS, M.; VAN RIJN, M.; VAN PAASSEN, R. Designing privacy-by-design. In: **Annual Privacy Forum**. Springer, Berlin, Heidelberg, p. 55-72, 2014.

(VEMOU; KARYDA, 2014) VEMOU, K.; KARYDA, M. Embedding privacy practices in social networking services. In: **proceedings of the 7th IADIS International Conference Information Systems**. p. 201-208, 2014.

(VENKATESH; BALA, 2008) VENKATESH, V.; BALA, H. Technology acceptance model 3 and a research agenda on interventions. **Decision sciences**, v. 39, n. 2, p. 273-315, 2008.

(VERSIONONE INC., 2015) VERSIONONE INC. **The 9th Annual State of Agile Survey. Annual State of Agile Survey**. Version 9, 2015.

(VERSIONONE INC., 2022) VERSIONONE INC. **The 16th Annual State of Agile Report**. Version 16, 2022.

(VESELI *et al.*, 2019) VESELI, F.; OLVERA, J. S.; PULLS, T.; RANNENBERG, K. Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In: **Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing**. p. 1475-1483, 2019.

(VIITANIEMI, 2017) VIITANIEMI, M. **Privacy by Design in Agile Software Development**. 2017. p. 49. Master of Science Thesis - Tampere University of Technology, Finland, 2017.

(WANG, 2003) WANG, L.; WU, G. Attribute reduction and information granularity. In: **6th World Multi conference on Systemics, Cybernetics and Informatics**. p. 32-37, 2003.

(WARREN; BRANDEIS, 1890) WARREN, S.; BRANDEIS, L. The right to privacy. **Harvard law review**, v. 4, n. 5, p. 193-220, 1890.

(WAZLAWICK, 2019) WAZLAWICK, R. **Engenharia de software: conceitos e práticas**. Elsevier Editora Ltda., 2019.

(WESTIN, 1967) WESTIN, A. F. Privacy and freedom Atheneum. **New York**, v. 7, p. 431–453, 1967.

(WIERINGA *et al.*, 2006) WIERINGA, R.; MAIDEN, N.; MEAD, N.; ROLLAND, C. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. **Requirements engineering**, v. 11, n. 1, p. 102-107, 2006.

(WOHLIN; AURUM, 2015) WOHLIN, C.; AURUM, A. Towards a decision-making structure for selecting a research design in empirical software engineering. **Empirical Software Engineering**, v. 20, p. 1427-1455, 2015.

(XUAN; WANG; LI, 2014) XUAN, X.; WANG, Y.; LI, S. Privacy requirements patterns for mobile operating systems. In: **2014 IEEE 4th International Workshop on Requirements Patterns (RePa)**. IEEE, p. 39-42, 2014.

(YIN, 2018) YIN, R. **Case study research and applications**. Thousand Oaks, CA: Sage, 2018.

APÊNDICE A – DOCUMENTAÇÃO UTILIZADA

A.1 Carta de Apresentação

Curitiba, <dia> de <mês> de <ano>.

Prezado(a) Senhor(a),

Venho, por meio desta, solicitar a sua autorização para a condução de um estudo de campo da tese de doutorado do aluno Vinícius Camargo Andrade, que está sendo desenvolvida sob minha orientação e coorientação das Professoras Drª Cinthia Obladen de Almendra Freitas e Drª Sheila Reinehr no Programa de Pós-Graduação em Informática da PUCPR.

O objetivo principal da pesquisa é entender como a privacidade de dados pessoais está sendo integrada ao desenvolvimento ágil de software e quais são as dificuldades associadas a esta integração.

A pesquisa será realizada por meio de entrevistas semiestruturadas, que visam coletar as informações necessárias para extrair resultados claros e concisos de como as organizações criam, transformam e armazenam os conhecimentos organizacionais, assim como quais tecnologias utilizam para tanto.

Gostaria, ainda, de afirmar o nosso compromisso em relação à confidencialidade das informações prestadas. Todos os dados serão tratados de forma a preservar a privacidade, tanto dos entrevistados, quanto da instituição. Nenhuma informação personalizada será publicada, a menos que autorizado formalmente pela organização. Um Termo de Compromisso de Utilização de Dados (TCUD) será assinado pelos pesquisadores, com termos a critério da organização.

Aguardamos o seu retorno e antecipadamente agradecemos pela colaboração.

Atenciosamente,

Andreia Malucelli, PhD
Programa de Pós-Graduação em Informática
Pontifícia Universidade Católica do Paraná – PUCPR.

A.2 Termo de Compromisso e Utilização de Dados (TCUD)

Nós, Vinícius Camargo Andrade, Andreia Malucelli, Cinthia Obladen de Almendra Freitas e Sheila Reinehr, abaixo assinado(s), pesquisadores envolvidos no projeto de *Privacy by Design Plug-in*: um *plugin* de processo de software para integração da privacidade de dados pessoais no desenvolvimento ágil de software, nos comprometemos a manter a confidencialidade sobre os dados coletados nas entrevistas, bem como a privacidade de seus conteúdos, como preconizam os Documentos Internacionais e as Resoluções 466/12 e 510/16, do Conselho Nacional de Saúde (CONEP).

Informo que os dados a serem coletados dizem respeito a colaboração com um estudo de caso o qual visa compreender como as organizações estão integrando a privacidade de dados pessoais ao desenvolvimento ágil de software e quais as dificuldades associadas a esta integração, ocorridos entre as datas de: <data de início> a <data de fim>.

Local, <dia> de <mês> de <ano>.

Envolvidos na manipulação e coleta dos dados:

Nome completo	CPF	Assinatura
Vinícius Camargo Andrade		
Andreia Malucelli		
Cinthia Obladen de Almendra Freitas		
Sheila Reinehr		

A.3 Termo de Consentimento Livre e Esclarecido

Você está sendo convidado(a) como voluntário(a) a participar do estudo sobre um *plugin* de processo de software, que tem como objetivo apoiar equipes ágeis na implementação dos princípios do *Privacy by Design* no processo de desenvolvimento de software, resultando em sistemas em conformidade com a legislação e menos suscetíveis a problemas relacionados à privacidade dos dados pessoais. Acreditamos que esta pesquisa seja importante porque poderá auxiliar pesquisadores no meio acadêmico ou profissionais da indústria durante o processo de desenvolvimento de software. Espera-se que os resultados obtidos apoiem as áreas de engenharia de requisitos, design e implementação de software, bem como todo o ciclo de vida do tratamento dos dados pessoais, como coleta, retenção, processamento, compartilhamento e eliminação dos dados.

PARTICIPAÇÃO NO ESTUDO

A sua participação no referido estudo será de colaborar com um estudo de caso o qual visa compreender como as organizações estão integrando a privacidade de dados pessoais ao desenvolvimento ágil de software e quais as dificuldades associadas a esta integração. Para isso, uma entrevista semiestruturada será realizada de maneira virtual utilizando a plataforma Google Meet (https://meet.google.com/). O tempo médio para na entrevista é, em média, 1 hora.

RISCOS E BENEFÍCIOS

Através deste Termo de Consentimento Livre e Esclarecido você está sendo alertado de que, da pesquisa a se realizar, não há benefício direto e/ou indireto ao entrevistado. Bem como, também que é possível que aconteçam os seguintes desconfortos ou riscos em sua participação, tais como: o participante pode se sentir-se constrangido em participar, ou, sentir efeitos de fadiga, pois o estudo tem duração média de uma hora. Neste caso, o participante poderá manifestar seu desconforto e abandonar a pesquisa a qualquer momento. Para minimizar tais riscos, nós pesquisadores tomaremos as seguintes medidas: dias e horários distintos serão marcados com cada participante individualmente e remotamente via e-mail e/ou por meio das plataformas

on-line (https://meet.google.com/). O objetivo do atendimento individual e virtual será minimizar impactos do COVID-19, bem como tornar o momento de entrevista mais confortável para todos os participantes. Assim, acredita-se que riscos ou efeitos de fadiga ou *stress* dos participantes serão minimizados em tal contexto.

SIGILO E PRIVACIDADE

Nós pesquisadores garantiremos a você que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, lhe identificar, será mantido em sigilo. Nós pesquisadores nos responsabilizaremos pela guarda e confidencialidade dos dados, bem como a não exposição de quaisquer informações em qualquer formato que possa indicar sua identidade.

AUTONOMIA

Nós lhe asseguramos assistência durante toda pesquisa, bem como garantiremos seu livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo e suas consequências, enfim, tudo o que você queira saber antes, durante e depois de sua participação. Também informamos que você pode se recusar a participar do estudo, ou retirar seu consentimento a qualquer momento, sem precisar justificar e sem qualquer prejuízo à assistência que vem recebendo.

RESSARCIMENTO E INDENIZAÇÃO

Caso tenha qualquer despesa decorrente da participação nesta pesquisa, tais como transporte, alimentação entre outros, haverá ressarcimento dos valores gastos na forma seguinte: mediante depósito em conta corrente. Também informamos que, na ocorrência de algum dano decorrente de sua participação no estudo, você será devidamente indenizado, conforme determina a lei.

CONTATO

Os pesquisadores envolvidos com o referido projeto são: Doutorando Vinícius Camargo Andrade (Pesquisador Responsável/Principal), orientado pela Profª Drª Andreia Malucelli e, coorientado pelas Professoras Drª Cinthia Obladen de Almendra Freitas e Drª Sheila Reinehr, na Pontifícia Universidade Católica do Paraná (PUCPR) e, com eles(as), você poderá manter contato pelos e-mails:

vcandrade@ppgia.pucpr.br, malu@ppgia.pucpr.br e cinthia.freitas@pucpr.br e sheila.reinehr@pucpr.br.

O Comitê de Ética em Pesquisa em Seres Humanos (CEP) é composto por um grupo de pessoas que estão trabalhando para garantir que seus direitos como participante de pesquisa sejam respeitados. Ele tem a obrigação de avaliar se a pesquisa foi planejada e se está sendo executada de forma ética. Se você achar que a pesquisa não está sendo realizada da forma como você imaginou ou que está sendo prejudicado de alguma forma, você pode entrar em contato com o Comitê de Ética em Pesquisa da PUCPR (CEP) pelo telefone (41) 3271-2103 entre segunda e sexta-feira das 08h00 às 17h30 ou pelo e-mail nep@pucpr.br.

DECLARAÇÃO

Declaro que li e entendi todas as informações presentes neste Termo de Consentimento Livre e Esclarecido e tive a oportunidade de discutir as informações deste termo. Todas as minhas perguntas foram respondidas e eu estou satisfeito com as respostas. Receberei uma via assinada e datada deste documento e igual a via assinada e datada que será arquivada pelo pesquisador responsável do estudo.

Enfim, tendo sido orientado quanto ao teor de todo o aqui mencionado e compreendido a natureza e o objetivo do já referido estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

Dados do participante da pesquisa	
Nome:	
Telefone:	
e-mail:	

Local, _____ de _____ de _____.

_____ _____

Assinatura do participante da pesquisa Assinatura do Pesquisador

A.4 Questionário de Caracterização de Perfil

Dados Pessoais (serão anonimizados):

Nome Completo: _____

E-mail para contato: _____

Questionário de Caracterização de Perfil:

Qual é o seu nível de formação?

( ) Graduação

( ) Especialização

( ) Mestrado

( ) Doutorado

Nome da Organização em que trabalha? _____

Qual é o Segmento de Mercado da Organização? _____

Qual é o seu Cargo/Função na Organização que atua? _____

Quanto tempo você tem de experiência na área? (exemplo: 8 anos e 5 meses) _____

Qual é o processo de desenvolvimento de software que a organização utiliza (exemplo: Scrum, Kanban, RUP, Cascata)? _____

Qual a sua experiência com desenvolvimento ágil?

( ) Eu nunca ouvi falar sobre desenvolvimento ágil.

( ) Eu tenho conhecimento teórico, já li sobre desenvolvimento ágil, mas nunca trabalhei desta forma.

( ) Minha experiência com desenvolvimento ágil é básica. Eu conheço os conceitos de Planning, Daily, Review, Retrospective e Sprints.

( ) Minha experiência com desenvolvimento ágil é Moderada. Já trabalhei em um time que usava desenvolvimento ágil, como por exemplo, Scrum, XP, Lean e Kanban.

( ) Minha experiência com desenvolvimento ágil é Avançada. Já atuei como gestor de times que usavam desenvolvimento ágil, como por exemplo, Scrum, XP, Lean e Kanban.

Qual a sua experiência com privacidade de dados pessoais?

( ) Eu nunca ouvi falar sobre privacidade de dados pessoais.

( ) Já li, de forma superficial, algo sobre privacidade de dados pessoais.

( ) Minha experiência com privacidade de dados pessoais é Básica. Eu fiz cursos introdutórios sobre o tema, mas não conheço em detalhes as leis que regulamentam o uso de dados pessoais.

( ) Minha experiência com privacidade de dados pessoais é Moderada. Eu fiz cursos introdutórios sobre o tema, eu conheço as leis e/ou regulamentos, mas nunca utilizei em nenhum projeto.

( ) Minha experiência com privacidade de dados pessoais é Avançada. Eu fiz cursos sobre o tema, conheço sobre as leis e/ou regulamentos e as utilizo na implementação de requisitos de privacidade em meus projetos de desenvolvimento de software.

A.5 Carta de Autorização da Instituição

TERMO DE AUTORIZAÇÃO

Este Termo de Autorização expressa a concordância da <NOME DA ORGANIZAÇÃO>, doravante denominada Organização Participante, em participar do estudo conduzido pelos pesquisadores Andreia Malucelli, Cinthia Obladen de Almendra Freitas, Sheila Reinehr e Vinícius Camargo Andrade, doravante denominados Pesquisadores, cujo objetivo compreender como a privacidade de dados pessoais está sendo integrada ao desenvolvimento ágil de software e quais são as dificuldades associadas a esta integração.

Os Pesquisadores se comprometem a:

- Portar-se com discrição em todos os momentos da pesquisa acadêmica, não comentando ou divulgando qualquer tipo de informação que tenha sido repassada de forma oral ou escrita.
- Não divulgar o nome da Organização Participante, em qualquer meio, a menos que expressamente autorizado por esta.
- Não divulgar, em qualquer meio, os dados e informações individualizados coletados durante o processo de pesquisa na Organização Participante.
- Divulgar, em formato de relatório técnico, artigos e apresentações, apenas os dados agregados, dos quais não se possa retirar ou inferir a identificação da Organização Participante ou de seus entrevistados de forma individualizada.
- Retornar para a Organização Participante as informações coletadas e analisadas, em formato de relatório individual e de forma agregada.

A assinatura abaixo expressa a concordância da Organização Participante em fazer parte do estudo cujo objetivo está supracitado.

<cidade>, <dia>/<mês>/<ano>

_____

NOME DO RESPONSÁVEL
NOME DA ORGANIZAÇÃO PARTICIPANTE

APÊNDICE B – CONJUNTO DE ESTUDOS PRIMÁRIOS SELECIONADOS

Quadro 10. Conjunto de estudos primários selecionados

Autor(es)	Título	Ano	Tipo de Pesquisa	Tipo de Publicação	Local da Publicação
Gaudino (2011)	Applied Sciences in Biomedical and ICT from the Perspective of the Patient's Right to Data Privacy and Security: Turning a Zero-Sum into a Positive-Sum Game	2011	Artigo de Opinião	Conferência	ISABEL
Kost *et al.* (2011)	Privacy Verification Using Ontologies	2011	Pesquisa de Validação	Conferência	ARES
Kung; Freytag; Kargl (2011)	Privacy-by-design in ITS Applications	2011	Artigo de Opinião	Conferência	WoWMoM
Alharbi; Zyngier; Hodkinson (2012)	An Evaluation of the Interaction Between Companies' Privacy Practices and User Information Privacy Concerns in the Success of Electronic Commerce	2012	Pesquisa de Avaliação	Conferência	EMCIS
Morton; Sasse (2012)	Privacy is a Process, Not a PET: A Theory for Effective Privacy Practice	2012	Proposta de Solução	Conferência	NSPW
Oetzel; Spiekermann (2012)	Privacy-by-Design Through Systematic Privacy Impact Assessment - A Design Science Approach	2012	Pesquisa de Validação	Conferência	ECIS
Spiekermann (2012)	The Challenges of Privacy by Design	2012	Artigo de Opinião	Journal	CACM
Jutla; Bodorik; Ali (2013)	Engineering Privacy for Big Data Apps with the Unified Modeling Language	2013	Proposta de Solução	Conferência	IEEE International Congress on Big Data
Chen; Williams (2013)	Grounding Privacy-by-Design for Information Systems	2013	Artigo Filosófico	Conferência	PACIS
Chandramouli; Arguedas; Izquierdo (2013)	Knowledge Modeling for Privacy-by-Design in Smart Surveillance Solution	2013	Artigo Filosófico	Conferência	AVSS
Le Métayer (2013)	Privacy by Design: A Formal Framework for the Analysis of Architectural Choices	2013	Pesquisa de Validação	Conferência	CODASPY
Van Rest *et al.* (2014)	Designing Privacy-by-Design	2014	Artigo Filosófico	Journal	APF
Vemou; Karyda (2014)	Embedding Privacy Practices in Social Networking Services	2014	Proposta de Solução	Conferência	ICIS
Rowan; Dehlinger (2014)	Encouraging Privacy by Design Concepts with Privacy Policy Auto-Generation in Eclipse (PAGE)	2014	Proposta de Solução	Conferência	eTX
Martín *et al.* (2014)	Engineering Privacy Requirements Valuable Lessons from Another Realm	2014	Artigo Filosófico	Conferência	ESPRE
Kung (2014)	PEARs: Privacy Enhancing ARchitectures	2014	Proposta de Solução	Journal	APF
Notario *et al.* (2014)	PRIPARE: A New Vision on Engineering Privacy and Security by Design	2014	Artigo Filosófico	Capítulo de Livro	CSP
Hoepman (2014)	Privacy Design Strategies	2014	Artigo Filosófico	Conferência	SEC
Stevovic *et al.* (2015a)	BPM Supported Privacy by Design for Cross-Organization Business Processes	2015	Proposta de Solução	Conferência	ICSOC

Stevovic *et al.* (2015b)	Enabling Privacy by Design in Medical Records Sharing	2015	Proposta de Solução	Capítulo de Livro	Reforming European Data Protection Law
Notario *et al.* (2015)	PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology	2015	Artigo Filosófico	Conferência	SPW
Hörbe; Hötzendorfer (2015)	Privacy by Design in Federated Identity Management	2015	Artigo Filosófico	Conferência	SPW
Kolkowska (2015)	Privacy Principles in Design of Smart Homes Systems in Elderly Care	2015	Artigo Filosófico	Conferência	HAS
Siljee (2015)	Privacy Transparency Patterns	2015	Proposta de Solução	Conferência	EuroPLoP
Kung; Jouvray; Coudert (2015)	SALT Frameworks to Tackle Surveillance and Privacy Concerns	2015	Proposta de Solução	Conferência	MODELSWARD
Colesky; Hoepman; Hillen (2016)	A Critical Analysis of Privacy Design Strategies	2016	Artigo Filosófico	Conferência	SPW
Hazeyama *et al.* (2016)	Literature Survey on Technologies for Developing Privacy-Aware Software	2016	Artigo Filosófico	Conferência	REW
Ali; Jutla; Bodorik (2016)	PIP: An Injection Pattern for Inserting Privacy Patterns and Services in Software	2016	Proposta de Solução	Journal	APF
Foukia; Billard; Solana (2016)	PISCES: A Framework for Privacy by Design in IoT	2016	Proposta de Solução	Conferência	PST
Degeling *et al.* (2016)	Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design	2016	Artigo Filosófico	Conferência	CIC
Colesky; Ghanavati (2016)	Privacy Shielding by Design - A Strategies Case for Near-Compliance	2016	Proposta de Solução	Conferência	REW
Perera *et al.* (2016)	Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms	2016	Proposta de Solução	Conferência	IoT
Aljohani *et al.* (2016)	Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act	2016	Artigo Filosófico	Conferência	HAS
Lenhard; Fritsch; Herold (2017)	A Literature Study on Privacy Patterns Research	2017	Artigo Filosófico	Conferência	SEAA
Alshammari; Simpson (2017b)	A UML Profile for Privacy-Aware Data Lifecycle Models	2017	Proposta de Solução	Journal	Computer Security
Blix; Elshekeil; Laoyookhong (2017)	Data Protection by Design in Systems Development: From Legal Requirements to Technical Solutions	2017	Proposta de Solução	Conferência	ICITST
Senarath; Arachchilage; Slay (2017)	Designing Privacy for You: A Practical Approach for User-Centric Privacy	2017	Proposta de Solução	Conferência	HAS
Caiza *et al.* (2017)	Organizing Design Patterns for Privacy: A Taxonomy of Types of Relationships	2017	Artigo Filosófico	Conferência	EuroPLoP
Alshammari; Simpson (2017c)	Personal Data Management: An Abstract Personal Data Lifecycle Model	2017	Proposta de Solução	Conferência	BPM
Hoel; Griffiths; Chen (2017)	The Influence of Data Protection and Privacy Frameworks on the Design of Learning Analytics Systems	2017	Artigo Filosófico	Conferência	LAK
Alshammari; Simpson (2017a)	Towards a Principled Approach for Engineering Privacy by Design	2017	Artigo Filosófico	Journal	APF
Guerriero *et al.* (2017)	Towards DevOps for Privacy-by-Design in Data-Intensive Applications: A Research Roadmap	2017	Pesquisa de Validação	Conferência	ICPE
Colesky *et al.* (2018)	A System of Privacy Patterns for User Control	2018	Artigo Filosófico	Conferência	SAC
Shishkov; Janssen (2018)	Enforcing Context-Awareness and Privacy-by-Design in the Specification of Information Systems	2018	Proposta de Solução	Conferência	BMSD

Trujillo e Mireles (2018)	Extending ISO/IEC 29110 Basic Profile with Privacy-by-Design Approach: A Case Study in the Health Care Sector	2018	Proposta de Solução	Conferência	QUATIC
Schneider (2018)	Is Privacy by Construction Possible?	2018	Artigo de Opinião	Conferência	ISoLA
Alshammari; Simpson (2018)	Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection	2018	Proposta de Solução	Conferência	WPES
Hadar *et al.* (2018)	Privacy by Designers: Software Developers' Privacy Mindset	2018	Pesquisa de Avaliação	Conferência	ICSE
Vaidya e Mouftah (2018)	Protecting the Privacy of Electricity Consumers in the Smart City	2018	Artigo Filosófico	Capítulo de Livro	Transportation and Power Grid in Smart Cities: Communication Networks and Services
Romanou (2018)	The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise	2018	Artigo Filosófico	Journal	CLSR
Galvez; Gurses (2018)	The Odyssey: Modeling Privacy Threats in a Brave New World	2018	Artigo Filosófico	Conferência	EuroS&PW
Rygge; Jøsang (2018)	Threat Poker: Solving Security and Privacy Threats in Agile Software Development	2018	Proposta de Solução	Conferência	NordSec
Senarath; Arachchilage (2018)	Why Developers Cannot Embed Privacy into Software Systems?: An Empirical Investigation	2018	Pesquisa de Avaliação	Conferência	EASE
Al-Momani *et al.* (2019)	A Privacy-Aware V-Model for Software Development	2019	Proposta de Solução	Conferência	SPW
Piras *et al.* (2019)	DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance	2019	Proposta de Solução	Conferência	TrustBus
Baldassarre *et al.* (2019)	Privacy Oriented Software Development	2019	Proposta de Solução	Conferência	QUATIC
Ahmadian; Strüber; Jürjens (2019)	Privacy-Enhanced System Design Modeling Based on Privacy Features	2019	Proposta de Solução	Conferência	SAC
Dodero *et al.* (2019)	Privacy-Preserving Reengineering of Model-View-Controller Application Architectures Using Linked Data	2019	Proposta de Solução	Journal	JWE
Bargh; Choenni (2019)	Towards Applying Design-Thinking for Designing Privacy-Protecting Information Systems	2019	Artigo Filosófico	Conferência	TPS-ISA
Sakul-Ung; Smanchat (2019)	Towards Privacy Framework in Software Development Projects and Applications: An Integrated Framework	2019	Proposta de Solução	Conferência	RI2C
Bu *et al.* (2020)	“Privacy by Design” implementation: Information System Engineers’ Perspective	2020	Pesquisa de Avaliação	Journal	IJIM
Tamburri (2020)	Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and its Evaluation	2020	Artigo Filosófico	Journal	ISJ
Perera *et al.* (2020)	Designing Privacy-Aware Internet of Things Applications	2020	Pesquisa de Validação	Journal	Information Sciences
Hatamian (2020)	Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers	2020	Artigo Filosófico	Journal	IEEE Access

Baldassarre *et al.* (2020)	Integrating Security and Privacy in Software Development	2020	Proposta de Solução	Journal	Software Quality Journal
Bugeja; Jacobsson (2020)	On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces	2020	Proposta de Solução	Journal	IFIP
Peixoto (2020)	Privacy Requirements Engineering in Agile Software Development: A Specification Method	2020	Proposta de Solução	Conferência	REFSQ
Semantha *et al.* (2021)	A Conceptual Framework to Ensure Privacy in Patient Record Management System	2021	Proposta de Solução	Journal	IEEE Access
Pedroza *et al.* (2021)	A Model-Based Approach to Realize Privacy and Data Protection by Design	2021	Proposta de Solução	Conferência	EuroS&PW
Amankona *et al.* (2021)	Integrating Privacy-By-Design in e-Health	2021	Proposta de Solução	Conferência	ICECET
Baldassarre *et al.* (2021)	Integrating Security and Privacy in HCD-Scrum	2021	Proposta de Solução	Conferência	CHItaly
Bu *et al.* (2021)	Motivating Information System Engineers' Acceptance of Privacy by Design in China: An Extended UTAUT Model	2021	Pesquisa de Avaliação	Journal	IJIM
Tahaei *et al.* (2021)	Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges	2021	Pesquisa de Avaliação	Conferência	CHI
Ayalon e Toch (2021)	User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes	2021	Pesquisa de Avaliação	Journal	International Journal of Human-Computer Studies
Righini *et al.* (2022)	A Privacy-Aware Zero Interaction Smart Mobility System	2022	Proposta de Solução	Journal	IEEE Access

APÊNDICE C – SÍNTESE DOS DADOS EXTRAÍDOS DOS ESTUDOS PRIMÁRIOS SELECIONADOS

Quadro 11. Dados extraídos dos estudos primários selecionados

Autor(es)	Título	Tipo de Contribuição	Área de Conhecimento de Engenharia de Software	Domínio da Aplicação	Modelo de Processo
Gaudino (2011)	Applied Sciences in Biomedical and ICT from the Perspective of the Patient's Right to Data Privacy and Security: Turning a Zero-Sum into a Positive-Sum Game	Teórico	Geral	Sistemas de Saúde	-
Kost *et al.* (2011)	Privacy Verification Using Ontologies	Modelo	Requisitos de Software	Sistemas de Transporte Inteligente	-
Kung; Freytag; Kargl (2011)	Privacy-by-design in ITS Applications	Teórico	Geral	Sistemas de Pedágio	Modelo Tradicional
Alharbi; Zyngier; Hodkinson (2012)	An Evaluation of the Interaction Between Companies' Privacy Practices and User Information Privacy Concerns in the Success of Electronic Commerce	Prática Profissional	Geral	E-commerce	-
Morton; Sasse (2012)	Privacy is a Process, Not a PET: A Theory for Effective Privacy Practice	Modelo	Requisitos de Software	Energia	-
Oetzel; Spiekermann (2012)	Privacy-by-Design Through Systematic Privacy Impact Assessment - A Design Science Approach	Método	Requisitos de Software	Geral	-
Spiekermann (2012)	The Challenges of Privacy by Design	Teórico	Geral	-	-
Jutla; Bodorik; Ali (2013)	Engineering Privacy for Big Data Apps with the Unified Modeling Language	Ferramenta	Requisitos de Software	Big Data	Modelo Tradicional
				Sistemas de Saúde	Processo Ágil
Chen; Williams (2013)	Grounding Privacy-by-Design for Information Systems	Teórico	Requisitos de Software	-	-
Chandramouli; Arguedas; Izquierdo (2013)	Knowledge Modeling for Privacy-by-Design in Smart Surveillance Solution	Modelo	Requisitos de Software	Sistemas de Vigilância	-
Le Métayer (2013)	Privacy by Design: A Formal Framework for the Analysis of Architectural Choices	Modelo	Projeto de Software	Sistemas de Pedágio	-
Van Rest *et al.* (2014)	Designing Privacy-by-Design	Teórico	Geral	-	Modelo Tradicional
					Modelo SIMILAR (BAHILL; GISSING, 1998)
					Modelo TOGAF (THE OPEN GROUP, 2021)
Vemou; Karyda (2014)	Embedding Privacy Practices in Social Networking Services	Modelo	Requisitos de Software	Serviços Online	-

Rowan; Dehlinger (2014)	Encouraging Privacy by Design Concepts with Privacy Policy Auto-Generation in Eclipse (PAGE)	Ferramenta	Construção de Software	-	-
Martín *et al.* (2014)	Engineering Privacy Requirements Valuable Lessons from Another Realm	Modelo	Requisitos de Software	-	-
Kung (2014)	PEARs: Privacy Enhancing ARchitectures	Padrão	Projeto de Software	Sistemas de Pedágio	-
Notario *et al.* (2014)	PRIPARE: A New Vision on Engineering Privacy and Security by Design	Teórico	Processo de Software	-	Genérico
Hoepman (2014)	Privacy Design Strategies	Padrão	Projeto de Software	-	Modelo Genérico de Desenvolvimento Incremental
Stevovic *et al.* (2015a)	BPM Supported Privacy by Design for Cross-Organization Business Processes	Método	Requisitos de Software	Sistemas de Saúde	Genérico
Stevovic *et al.* (2015b)	Enabling Privacy by Design in Medical Records Sharing	Método	Processo de Software	Sistemas de Saúde	Modelo Genérico de Desenvolvimento Incremental
Notario *et al.* (2015)	PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology	Método	Processo de Software	-	-
Hörbe; Hötzendorfer (2015)	Privacy by Design in Federated Identity Management	Teórico	Requisitos de Software	Sistemas de Autenticação	-
Kolkowska (2015)	Privacy Principles in Design of Smart Homes Systems in Elderly Care	Teórico	Requisitos de Software	Sistemas de Saúde	-
Siljee (2015)	Privacy Transparency Patterns	Padrão	Projeto de Software	Sistemas de Saúde	-
Kung; Jouvray; Coudert (2015)	SALT Frameworks to Tackle Surveillance and Privacy Concerns	Modelo	Projeto de Software	Sistema de Vigilância	-
Colesky; Hoepman; Hillen (2016)	A Critical Analysis of Privacy Design Strategies	Padrão	Projeto de Software	-	-
Hazeyama *et al.* (2016)	Literature Survey on Technologies for Developing Privacy-Aware Software	Teórico	Geral	-	-
Ali; Jutla; Bodorik (2016)	PIP: An Injection Pattern for Inserting Privacy Patterns and Services in Software	Padrão	Construção de Software	Sistemas Bancário	-
Foukia; Billard; Solana (2016)	PISCES: A Framework for Privacy by Design in IoT	Modelo	Projeto de Software	Internet of Things	-
Degeling *et al.* (2016)	Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design	Modelo	Projeto de Software	Geral	-
Colesky; Ghanavati (2016)	Privacy Shielding by Design - A Strategies Case for Near-Compliance	Padrão	Requisitos de Software	Sistemas de Saúde	-
Perera *et al.* (2016)	Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms	Modelo	Projeto de Software	Internet of Things	-
Aljohani *et al.* (2016)	Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act	Padrão	Requisitos de Software	Sistemas de Saúde	-
Lenhard; Fritsch; Herold (2017)	A Literature Study on Privacy Patterns Research	Teórico	Geral	-	-

Alshammari; Simpson (2017b)	A UML Profile for Privacy-Aware Data Lifecycle Models	Ferramenta	Requisitos de Software	Sistemas de Pedágio	-
Blix; Elshekeil; Laoyookhong (2017)	Data Protection by Design in Systems Development: From Legal Requirements to Technical Solutions	Modelo	Processo de Software	-	-
Senarath; Arachchilage; Slay (2017)	Designing Privacy for You: A Practical Approach for User-Centric Privacy	Método	Processo de Software	Serviços Online	Unified Process (UP)
Caiza *et al.* (2017)	Organizing Design Patterns for Privacy: A Taxonomy of Types of Relationships	Padrão	Projeto de Software	-	-
Alshammari; Simpson (2017c)	Personal Data Management: An Abstract Personal Data Lifecycle Model	Modelo	Requisitos de Software	-	-
Hoel; Griffiths; Chen (2017)	The Influence of Data Protection and Privacy Frameworks on the Design of Learning Analytics Systems	Modelo	Requisitos de Software	Educação	-
Alshammari; Simpson (2017a)	Towards a Principled Approach for Engineering Privacy by Design	Método	Requisitos de Software	-	-
Guerriero *et al.* (2017)	Towards DevOps for Privacy-by-Design in Data-Intensive Applications: A Research Roadmap	Ferramenta	Construção de Software	Big Data	-
Colesky *et al.* (2018)	A System of Privacy Patterns for User Control	Padrão	Projeto de Software	-	-
Shishkov; Janssen (2018)	Enforcing Context-Awareness and Privacy-by-Design in the Specification of Information Systems	Modelo	Projeto de Software	Geral	Unified Process (UP)
Trujillo e Mireles (2018)	Extending ISO/IEC 29110 Basic Profile with Privacy-by-Design Approach: A Case Study in the Health Care Sector	Modelo	Processo de Software	Sistemas de Saúde	Modelo Tradicional
Schneider (2018)	Is Privacy by Construction Possible?	Teórico	Geral	-	-
Alshammari; Simpson (2018)	Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection	Modelo	Processo de Software	Sistemas de Pedágio	-
Hadar *et al.* (2018)	Privacy by Designers: Software Developers' Privacy Mindset	Prática Profissional	Geral	Geral	-
Vaidya e Mouftah (2018)	Protecting the Privacy of Electricity Consumers in the Smart City	Teórico	Requisitos de Software	Energia	Modelo Tradicional Processo Ágil
Romanou (2018)	The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise	Teórico	Geral	Sistemas de Autenticação Sistemas de Saúde Sistemas de Vigilância	-
Galvez; Gurses (2018)	The Odyssey: Modeling Privacy Threats in a Brave New World	Teórico	Geral	-	Processo Ágil
Rygge; Jøsang (2018)	Threat Poker: Solving Security and Privacy Threats in Agile Software Development	Método	Requisitos de Software	-	Processo Ágil
Senarath; Arachchilage (2018)	Why Developers Cannot Embed Privacy into Software Systems?: An Empirical Investigation	Prática Profissional	Geral	Sistemas de Saúde	-

Al-Momani *et al.* (2019)	A Privacy-Aware V-Model for Software Development	Modelo	Processo de Software	-	Modelo V
Piras *et al*. (2019)	DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance	Ferramenta	Projeto de Software	Energia Sistemas de Saúde	-
Baldassarre *et al.* (2019)	Privacy Oriented Software Development	Método	Processo de Software	Serviços Online	Modelo Tradicional
Ahmadian; Strüber; Jürjens (2019)	Privacy-Enhanced System Design Modeling Based on Privacy Features	Método	Projeto de Software	Geral	-
Dodero *et al.* (2019)	Privacy-Preserving Reengineering of Model-View-Controller Application Architectures Using Linked Data	Método	Construção de Software	Serviços Online	-
Bargh; Choenni (2019)	Towards Applying Design-Thinking for Designing Privacy-Protecting Information Systems	Modelo	Requisitos de Software	Geral	-
Sakul-Ung; Smanchat (2019)	Towards Privacy Framework in Software Development Projects and Applications: An Integrated Framework	Modelo	Processo de Software	-	Modelo Tradicional
Bu *et al.* (2020)	"Privacy by Design" implementation: Information System Engineers' Perspective	Prática Profissional	Geral	-	-
Tamburri (2020)	Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and its Evaluation	Modelo	Requisitos de Software	-	-
Perera *et al.* (2020)	Designing Privacy-Aware Internet of Things Applications	Modelo	Projeto de Software	Internet of Things	-
Hatamian (2020)	Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers	Modelo	Geral	Sistemas de Saúde	-
Baldassarre *et al.* (2020)	Integrating Security and Privacy in Software Development	Método	Processo de Software	Serviços Online	Modelo Genérico de Desenvolvimento Incremental
Bugeja; Jacobsson (2020)	On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces	Método	Requisitos de Software	Internet of Things	-
Peixoto (2020)	Privacy Requirements Engineering in Agile Software Development: A Specification Method	Método	Requisitos de Software	-	Processo Ágil
Semantha *et al.* (2021)	A Conceptual Framework to Ensure Privacy in Patient Record Management System	Modelo	Projeto de Software	Sistemas de Saúde	-
Pedroza *et al.* (2021)	A Model-Based Approach to Realize Privacy and Data Protection by Design	Método	Processo de Software	Geral	-
Amankona *et al.* (2021)	Integrating Privacy-By-Design in e-Health	Modelo	Projeto de Software	Sistemas de Saúde	-
Baldassarre *et al.* (2021)	Integrating Security and Privacy in HCD-Scrum	Método	Processo de Software	Geral	Processo Ágil
Bu *et al.* (2021)	Motivating Information System Engineers' Acceptance of Privacy by Design in China: An Extended UTAUT Model	Prática Profissional	Geral	-	-
Tahaei *et al.* (2021)	Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges	Prática Profissional	Geral	-	-

Ayalon e Toch (2021)	User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes	Teórico	Geral	-	-
Righini *et al*. (2022)	A Privacy-Aware Zero Interaction Smart Mobility System	Ferramenta	Construção de Software	Sistemas de Transporte Inteligente	-

APÊNDICE D – ESTUDOS DE CASOS

D.1 Organização A

- **Atividades da organização:** Varejo.
- **Caracterização da Organização:** Empresa de Capital Aberto.
- **Número de Colaboradores:** 1.000 – 9.999.
- **Área de atendimento ao cliente:** Diversas áreas.

D.1.1 Perfis dos Colaboradores

Foram entrevistados dois colaboradores da Organização A. Suas respectivas funções, experiências, tempo de organização e duração da entrevista estão descritos no Quadro 12.

Quadro 12. Organização A - Perfis dos Colaboradores.

Organização A	Função/Cargo	Tempo de trabalho na Organização	Tempo de Experiência (desde a graduação)	Duração da Entrevista
Colaborador A	Gerente de Produtos Digitais e Transformação	4 anos e 7 meses	8 anos	00:26:55
Colaborador B	Analista Especialista de Integrações	3 anos e 8 meses	10 anos	00:31:25

D.1.2 Descrição dos Pontos de Análise

A atividade principal da organização se concentra no domínio de varejo, atendendo tanto ao mercado brasileiro quanto externo. Apesar do desenvolvimento de software não ser a principal atividade exercida pela organização, ela possui um departamento específico à implementação e manutenção de produtos de software da própria organização.

Recentemente os gestores da organização definiram o modelo Scrum como base para o processo de desenvolvimento e manutenção dos produtos de software. Porém, os times de desenvolvimento possuem autonomia para adaptar o modelo de acordo com a necessidade, respeitando as datas de implantação e as cerimônias do Scrum, como por exemplo, *Sprint Planning*, *Daily Meeting*, *Sprint Review Meeting* e *Sprint Retrospective*.

Além disso, constatou-se que atualmente a organização possui o cargo de *Product Owner*, entretanto, há uma discussão em andamento para que os colaboradores deste cargo assumam responsabilidades extras e, consequentemente, sejam promovidos a *Product Manager*. No entanto, não foi constatado etapas responsáveis pela integração da privacidade de dados pessoais ao processo de desenvolvimento de software da organização. Sendo assim, o **Ponto de Análise 01 não foi encontrado na organização**. O Quadro 13 apresenta as citações dos colaboradores da Organização A referente ao Ponto de Análise 01.

Quadro 13. Descrição do Ponto de Análise 01 na Organização A.

Ponto de Análise	Resultado
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software. *(Colaborador A) "[...] a gente usa o Scrum, mas não é nada rígido. Então, tem variação de tempo entre os times. Aqui os times tem autonomia para editar em cima de um processo pré-existente."* *(Colaborador B) "a gente usa as reuniões diárias, as meetings das sprints, como por exemplo, planning, review e retrospective."* *(Colaborador A) "hoje o que a gente tem são Product Owners, como cargo. Mas que a gente está começando a dar uma responsabilidade de Product Manager para ele. Nosso objetivo em curto prazo, médio prazo, vamos dizer assim. Em 2023 a gente não ter mais o papel nem cargo de PO, Product Owner, só de Product Manager."* *(Entrevistador) "Há Processos específicos utilizados na organização para a integração da privacidade de dados pessoais?"* *(Colaborador A) "Não."* *(Entrevistador) Existe então, dentro desse processo adaptado que você me falou, scrum, kanban, tanto faz, mas existe algum processo específico que integra a privacidade de dados nos processos ágeis que vocês usam?* *(Colaborador B) Não, não. Eu nunca ouvi falar de nada específico.*	○

Constatou-se que os times de desenvolvimento são constituídos com perfis multidisciplinares, como designer, desenvolvedor, testador, entre outros. Porém, não há um especialista em privacidade de dados pessoais na integração destes times.

Verificou-se que a organização possui apenas os perfis necessários para estar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a), denominados de agentes de tratamento de dados. Atualmente, a organização está passando por uma reestruturação em que os agentes de tratamento de dados prestarão consultorias aos times de desenvolvimento. Quando uma determinada equipe necessitar solucionar problemas referentes ao tratamento de dados pessoais, estes agentes serão alocados a esta equipe a fim de esclarecer dúvidas e minimizar as incertezas do projeto. Desta maneira, o **Ponto de Análise 02 não foi encontrado na organização**. O Quadro 14 descreve as citações dos colaboradores referentes ao Ponto de Análise 02.

Quadro 14. Descrição do Ponto de Análise 02 na Organização A.

Ponto de Análise	Resultado
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software. *(Colaborador A) "os times possuem colaboradores de diversas áreas. Eu tenho gente responsável pela interface do usuário, pelo desenvolvimento, pelo teste. Mas a gente não tem nenhuma iniciativa para colocar gente de privacidade nos times."* *(Entrevistador) "E tem algum especialista em privacidade de dados dentro desses times [de desenvolvimento]?"* *(Colaborador B) "Não tem, não tem."* *(Colaborador A) "eu tenho isso na minha equipe [pessoas responsáveis pela privacidade de dados], mas apartado dos times. A gente tem um DPO, que tem mais uma ou duas pessoas de segurança abaixo."* *(Colaborador A) "Esse DPO vai fazer uma maior conscientização das pessoas. [...] O que a gente está construindo agora é o DPO ser mais ativo nos times."* *(Colaborador A) "No cadastro a gente tem, obviamente, as diretrizes da LGPD. Então, a gente faz a coleta opt-in. Para armazenamento a gente também segue os padrões [...] da LGPD. De criptografia e tudo mais. E para acesso a gente também controla via processo de liberação de acesso à plataforma."* *(Colaborador B) "[os responsáveis pela privacidade de dados pessoais] atendem sob demanda a gente. E, provavelmente, tem as próprias demandas deles."*	○

Identificou-se que os colaboradores da organização, ao serem admitidos, realizam diversos cursos, entre eles o de privacidade de dados pessoais e Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018a). Entretanto, não são cursos específicos com a finalidade de formar um colaborador especialista em privacidade de dados pessoais.

Dado a demanda na área de privacidade de dados pessoais, a organização possui uma iniciativa para que os agentes de tratamento de dados pessoais sejam mais ativos nos times de desenvolvimento, promovendo uma maior conscientização sobre a privacidade de dados pessoais para que os próprios colaboradores tomem os devidos cuidados no momento da implementação de funcionalidades que envolvam o ciclo de vida do dado. Entretanto, atualmente isso não ocorre. Desse modo, o **Ponto de Análise 03 foi encontrado parcialmente na organização**. O Quadro 15 exibe as citações dos colaboradores referentes ao Ponto de Análise 03.

Quadro 15. Descrição do Ponto de Análise 03 na Organização A.

Ponto de Análise	Resultado
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização. *(Colaborador A) "quando eu entro, eu tenho um curso de privacidade que eu tenho que assistir. [...] No onboard de colaboradores você tem um curso lá daqueles padrões quando você entra em uma companhia tem vários cursinhos que você tem que fazer, um deles é de privacidade de dados. [...] Tem vários cursos lá, de LGPD, de privacidade."* *(Colaborador B) "a gente tem uma plataforma de capacitação interna também. Segurança. Enfim, né? Boas práticas. [...] Você entra na empresa, tem uma trilha lá para fazer [os cursos]."* *(Colaborador B) "a gente não recebeu nenhum tipo de capacitação para desenvolver olhando para a segurança de dados. O que a gente tem são desenvolvedores bem sêniors que às vezes já sabem o que funciona melhor."* *(Colaborador A) "isso [uma equipe especializada em privacidade de dados pessoais] a gente está estruturando para começar a cursar. Executando hoje não. A gente está estruturando essa equipe [de privacidade de dados pessoais] para fazer esse treinamento."* *(Colaborador A) "É um processo que a gente está aprendendo ainda. Tudo isso está sendo criado nos últimos 6 meses."*	◐

Segundo os colaboradores entrevistados, verificou-se que a organização não possui e/ou utiliza nenhuma ferramenta que auxilia o time de desenvolvimento na

detecção de vulnerabilidades e implementações de requisitos relacionados à privacidade de dados pessoais.

A preocupação da organização com questões relacionadas à privacidade de dados pessoais ainda é muito recente e, atualmente, a alta gerência está discutindo uma restruturação nas equipes e aquisições de ferramentas que auxiliem na integração da privacidade de dados pessoais ao desenvolvimento de software. Com isso, o **Ponto de Análise 04 não foi encontrado na organização**. O Quadro 16 aborda as citações dos colaboradores referentes ao Ponto de Análise 04.

Quadro 16. Descrição do Ponto de Análise 04 na Organização A.

Ponto de Análise	Resultado
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software. *(Colaborador A) "De privacidade, hoje não [temos ferramentas]. A gente está subindo agora para olhar qualidade, vai olhar um pouco de vulnerabilidade. Mas hoje, especificamente [de privacidade de dados pessoais], ainda não."* *(Colaborador B) "que eu saiba, não [temos ferramentas de privacidade de dados pessoais]."*	○

Apesar de atualmente a organização não contar com especialistas em privacidade de dados pessoais nos times de desenvolvimento, processos de desenvolvimento integrando a privacidade de dados pessoais e ferramentas que auxiliam a equipe técnica, a alta gerência reconhece a importância das questões da privacidade de dados e está investindo em restruturações, contratações e aquisições para se adequar à nova realidade da legislação e mercado.

Como maneira de minimizar as chances de ocorrerem falhas relativas à privacidade de dados pessoais, há um cuidado do time de desenvolvimento em reconhecer todos os usuários que interagirão com o sistema, bem como realizar testes de aceitação, denominadas *Proof of Concept* (POC), nas quais as opiniões dos usuários são coletadas e impactam diretamente como o software é desenvolvido.

Ainda, segundo os colaboradores, as demandas respectivas ao produto de software são priorizadas considerando os ritos do Scrum, sendo o time de desenvolvimento autônomo para priorizar as atividades pendentes. Porém, esta

autonomia não pode contrariar a LGPD. Neste caso, quando há riscos relativos à privacidade de dados pessoais, o produto de software não é implantado enquanto os riscos não forem totalmente sanados. Portanto, o **Ponto de Análise 05 não foi encontrado na organização**. O Quadro 17 destaca as citações dos colaboradores em relação ao Ponto de Análise 05.

Quadro 17. Descrição do Ponto de Análise 05 na Organização A.

Ponto de Análise	Resultado
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software. *(Colaborador A) "[o fomento se dá por] ter construído essa estrutura, [...], trazer conhecimento e pessoas e dar investimento. Hoje eu cuido de 1/3 do investimento da empresa como um todo. 1/3 do investimento da empresa está na minha área."* *(Colaborador A) "O mesmo para a privacidade. A gente contratou e estruturou uma área. Como a alta liderança apoia é investimento, grana e tempo."* *(Colaborador B) "a nossa gestão tem endossado de forma firme isso. É tipo um hiperativo para todo mundo agora se capacitar."* *(Colaborador A) "[os usuários] são [envolvidos nas etapas de desenvolvimento]. Ou fazendo POC com eles ou usando um processo de validação. [...] Peço para meu time ligar para eles, fazer uma videoconferência."* *(Colaborador B) "a gente faz uma etapa de mapeamento de papéis e responsabilidades, [...] tanto para usuários finais quanto para usuários do sistema."* *(Entrevistador) "Eles [os usuários] são envolvidos no processo de desenvolvimento?" (Colaborador B) "Sim, totalmente. Sempre na fase de homologação."* *(Colaborador A) "Agrega valor gerado na ponta [no produto final], não tenho certeza. Se ela enxerga como valor. Mas acho que ela enxerga como necessidade: 'Precisamos seguir as diretrizes de privacidade do país'. [...] Então a gente olha isso com viés jurídico, mais pela adequação as regras do que necessariamente por um 'enxergar valor'."* *(Colaborador A) "como eles [os times de desenvolvimento] tem uma autonomia, existe uma diretriz que não pode subir coisas que firam a LGPD, por exemplo. [...] Nessa linha [os gestores se preocupam com a privacidade do usuário] muito mais pelo cumprimento da regra do que pelo valor [do produto]."*	

D.1.3 Análise de Proposições

Para a Proposição 1 definiu-se quatro pontos de análise. O primeiro está relacionado a existência de processos sistematizados que visam integrar a privacidade de dados pessoais ao desenvolvimento ágil de software. Durante a análise verificou-se que, apesar da organização possuir um processo de desenvolvimento ágil de software, a privacidade de dados pessoais não é parte deste processo.

O segundo e terceiro pontos de análise dizem respeito a integração de especialistas em privacidade de dados pessoais nos times de desenvolvimento e o conhecimento, por parte da equipe técnica, em privacidade de dados. Neste contexto, verificou-se que a equipe é formada por profissionais multidisciplinares, porém, não há um especialista em privacidade de dados. Entretanto, os colaboradores, ao serem contratados, fazem diversos cursos admissionais, entre eles, de privacidade de dados pessoais.

Com relação ao quarto ponto de análise, constatou-se que a organização não utiliza ferramentas que auxiliam na detecção de vulnerabilidades e implementações de requisitos relacionados à privacidade de dados pessoais.

Com base nas evidências encontradas é possível afirmar que a deficiência do time de desenvolvimento, no que diz respeito ao conhecimento em privacidade de dados pessoais, e o não uso de ferramentas que os auxiliem na detecção e correção de falhas relacionadas ao tema, dificultam a integração da privacidade de dados pessoais nas atividades do processo ágil de desenvolvimento de software da organização. Por isso, a **Proposição 1 foi considerada verdadeira**. O Quadro 18 apresenta a análise da Proposição 1 na Organização A.

Quadro 18. Análise da Proposição 1 na Organização A.

Análise da Proposição	Resultado
Proposição 1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	○
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	○
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	◐
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	○

Para a Proposição 2 considerou apenas um ponto de análise, no qual constatou-se que a organização está realizando uma reestruturação e contratação de profissionais capacitados a fim de sanar os problemas relacionados à privacidade de dados pessoais. Isso está ocorrendo por meio do reconhecimento da alta gerência da organização sobre a importância de requisitos de privacidade e segurança da informação, principalmente após a implantação da LGPD. Dessa maneira, a **Proposição 2 foi considerada não verdadeira**. O Quadro 19 destaca a análise da Proposição 2 na Organização A.

Quadro 19. Análise da Proposição 2 na Organização A.

Análise da Proposição	Resultado
Proposição 2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	○
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	○

D.2 Organização B

- **Atividades da organização:** Serviços financeiros.
- **Caracterização da Organização:** Empresa de Capital Aberto.
- **Número de Colaboradores:** 1.000 – 9.999.
- **Área de atendimento ao cliente:** Diversas áreas.

D.2.1 Perfis dos Colaboradores

Neste estudo entrevistou-se dois colaboradores da Organização B. Suas respectivas funções, experiências, tempo de organização e duração da entrevista são descritos no Quadro 20.

Quadro 20. Organização B - Perfis dos Colaboradores.

Organização B	Função/Cargo	Tempo de trabalho na Organização	Tempo de Experiência (desde a graduação)	Duração da Entrevista
Colaborador C	Engenheiro de Software Sênior	5 anos e 3 meses	12 anos	00:39:52
Colaborador D	Analista de Qualidade	3 anos e 4 meses	12 anos	00:39:06

D.2.2 Descrição dos Pontos de Análise

A Organização B é uma organização do setor financeiro que desenvolve soluções para inovações para este segmento. Apesar da atividade principal da organização não ser a comercialização de software, os produtos de softwares desenvolvidos pela organização são de extrema importância, uma vez que todas as operações realizadas pelos seus clientes ocorrem por meio dos aplicativos mantidos pela organização.

Para o desenvolvimento e manutenção de seus produtos de software a organização utiliza o modelo Scrum, incluindo todos os ritos como, *sprint planning*, *daily meeting*, *sprint review* e *sprint retrospective*. Constatou-se que há papéis

específicos na equipe voltados ao produto da organização. Estes colaboradores possuem a função de realizar levantamento de questões relacionadas a estratégia da organização. Uma vez identificadas as necessidades de mercado, tanto o time técnico quanto o time de negócios, realizam o refinamento e priorização destes requisitos para iniciar o desenvolvimento em *sprints*.

Entretanto, não foi constatado etapas e/ou atividades sistemáticos para a identificação e solução de questões que envolvem a privacidade de dados pessoais. Segundo os colaboradores entrevistados, vulnerabilidades desta natureza são identificadas pelo próprio time de desenvolvimento no momento da elicitação e implementação de requisitos e, em alguns casos, o setor jurídico da organização é consultado a fim de garantir que a legislação vigente está sendo cumprida. Portanto, o **Ponto de Análise 01 não foi encontrado na organização**. O Quadro 21 aborda as citações dos colaboradores da Organização B referente ao Ponto de Análise 01.

Quadro 21. Descrição do Ponto de Análise 01 na Organização B.

Ponto de Análise	Resultado
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software. *(Colaborador C) "A gente trabalha com Scrum. [...] Tem todos os ritos. A gente tem planning, daily, tem review, tem retro."* *(Colaborador D) Sim, sim, todas as cerimônias [do scrum] são seguidas.* *(Colaborador C) "[...] existem pessoas do papel específico muito mais voltados para o produto e a principal missão destas pessoas é justamente trazer, entender dentro da missão do time, o que deve ser feito para a empresa, o que vai trazer mais valor."* *(Colaborador D) "A gente tem, dentro da nossa squad, da nossa equipe, tem pessoas que são voltadas para produto. Elas fazem primeiro o levantamento de questões de mercado, de priorização de acordo com a estratégia da empresa. A partir disso, feito essa priorização, uma demanda um pouco mais lapidada chega para os times e aí a gente faz um refinamento daquele tema [...]. A partir disso a gente vai conversando para entender cada vez mais, já vai começando a fazer um desenho de solução e, depois disso, posso te dizer que durante o refinamento, a gente faz divisões de histórias para conseguir pensar em entregas parciais de desenvolvimento e, depois disso, aí vem a o desenvolvimento em si. Mas aí depende muito mais de priorização sobre o que vai entrar em cada sprint para ser desenvolvido."* *(Colaborador C) "Hoje, os profissionais, principalmente lá [na organização], eles têm muita maturidade quanto esse tipo de situação [de identificar questões relacionadas a privacidade de dados pessoais], então eles mesmos já têm essa maturidade para saber: 'a gente está se envolvendo com um dado específico, um dado sensível que pode estar afetando a LGPD, esse tipo de coisa.', e eu sei que eles trabalham nesse tipo de caso até com o time jurídico até para entender quais são as complicações que tem."*	○

(Colaborador D) "[questões de privacidade de dados estão contidas] no fluxo de desenvolvimento, ela está embutida ali pela consciência dos desenvolvedores de não prover ou de cuidar desse tipo de informação." *(Colaborador C) "[...] essas decisões de refinamento é feita com o time todo. Não só o time técnico, mas o time de negócios também. [...] O pessoal já consegue, a experiência já faz entender que existe um risco [de privacidade de dados]."*	

Constatou-se que os times de desenvolvimento da organização são formados por colaboradores com perfis multidisciplinares. Não há nas equipes especialistas, como por exemplo, designers, desenvolvedor *back-end*, testador, entre outros. Conforme mencionado pelos colaboradores, os membros na equipe possuem conhecimento de todas as áreas necessárias para o desenvolvimento do produto, tanto relacionadas a detalhes técnicos, como linguagens de programação, ferramentas, *frameworks*, entre outros, quanto de leis e regulamentos, para incluir ao software os requisitos não funcionais, como privacidade de dados e segurança da informação. Dessa maneira, o **Ponto de Análise 02 não foi encontrado na organização**. O Quadro 22 destaca as citações dos colaboradores referentes ao Ponto de Análise 02.

Quadro 22. Descrição do Ponto de Análise 02 na Organização B.

Ponto de Análise	Resultado
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software. *(Colaborador C) "a ideia é que eles [os times] sejam cada vez mais multifuncionais. Então, é mais difícil você ver um cara que seja só back-end, o que ele seja só front-end. A ideia é que ele consiga navegar um pouco por cada uma dessas habilidades. [...] Você também tem que navegar por arquitetura. Então, cada vez mais se pede esse profissional full-cicle."* *(Colaborador D) "[as equipes são formadas por] desenvolvedores. Eles também têm a função de teste. Não tem segmentado ali [na organização] uma parte de QA [Quality Assurance]. Os devs mesmo codam e avaliam aquilo."* *(Colaborador D) "não, não tem alguém alocado especificamente [para privacidade de dados pessoais], porque isso está embutido dentro do fluxo de desenvolvimento. Quem está codificando precisa [...] ter isso em mente [questões de privacidade de dados pessoais] para não quebrar ou não infringir alguma coisa [lei/regulamento] alí."* *(Colaborador C) "[...] essa habilidade em lidar com privacidade de dados talvez seja mais um ponto que seja pedido para os profissionais de maneira geral e não especialista."*	○

Segundo os colaboradores entrevistados, a equipe técnica da organização recebe cursos específicos para a compreensão e implementação da LGPD. Porém, estes cursos não possuem o intuito de formar especialistas em privacidade de dados pessoais, pois o setor jurídico na organização se encarrega em sanar possíveis dúvidas no momento do desenvolvimento do produto de software.

Constatou-se que a organização fomenta e investe na atualização de seus colaboradores por meio de cursos e treinamentos em diversas áreas, inclusive de privacidade de dados e desenvolvimento ágil de software. Entretanto, devido à alta demanda pelos produtos, os colaboradores optam por fazer cursos relacionados as linguagens e tecnologias utilizadas no desenvolvimento de software a cursos voltados a privacidade de dados pessoais.

Cientes deste problema, a organização estabelece práticas que visam resguardar a privacidade de dados pessoais de seus clientes e devem ser seguidas pelos times de desenvolvimento. Além disso, há uma cultura na organização em que tópicos relacionados aos produtos, entre eles, privacidade de dados pessoais, são discutidos em fóruns nos quais os engenheiros de software trocam informações. Há também uma atividade chamada de *Review*, na qual um colaborador avalia as atividades desenvolvidas por outro, podendo solicitar alterações caso necessário. Sendo assim, o **Ponto de Análise 03 foi encontrado parcialmente na organização**. O Quadro 23 apresenta as citações dos colaboradores referentes ao Ponto de Análise 03.

Quadro 23. Descrição do Ponto de Análise 03 na Organização B.

Ponto de Análise	Resultado
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização. *(Colaborador C) "Iniciativa específica para a privacidade de dados, eu diria que não. Eu diria que existe um cuidado maior para a LGPD."* *(Colaborador D) "[os especialistas são alocados nos times] sob demanda. [...] são pessoas do setor jurídico que dão consultorias internas."* *(Colaborador D) "investimento em treinamento existe. É muito mais a questão da empresa querer que o seus colaboradores gastem um tempo nisso. [...] Ela já dedica parte do seu investimento para o desenvolvimento técnico."* *(Colaborador C) "[a organização] fomenta você buscar conhecimento de maneira geral com acesso a plataformas que até tem esse tipo de curso [de privacidade de dados]. Mas, sinceramente [...] eu acho improvável alguém parar para estudar isso [cursos relacionados a privacidade de dados]. Não que não seja um tema importante,*	◐

[...] mas na hora que você precisa priorizar entre estudar uma coisa e outra, eu não sei se essa seria a prioridade das pessoas." *(Colaborador C) "Material interno ajuda a fomentar a cultura de desenvolvimento. A gente tem vários fóruns entre engenheiros mesmo e vez ou outra alguma prática de segurança e privacidade acaba surgindo."* *(Colaborador C) "Toda hora tem o review que você precisa fazer de outra pessoa. Se você vê alguma coisa que você entende que está fora de um padrão, você vai falar para a pessoa, vai colocar um comentário pedindo para que aquilo seja corrigido."* *(Colaborador D) "é revisado internamente pela mesma equipe. Então outros desenvolvedores precisam ter a mesma preocupação que esse desenvolvedor que codificou teve na hora de codificar."*	

Os colaboradores mencionaram que há uma preocupação da organização com questões relacionadas à segurança da informação, em que ocorrem testes periódicos de possíveis vulnerabilidades no software. Porém, não se constatou a mesma preocupação da organização com questões relacionadas à privacidade de dados pessoais, visto que a organização não utiliza nenhuma ferramenta que auxilia o time de desenvolvimento na detecção de vulnerabilidades e implementações de requisitos relacionados a este requisito. Desse modo, o **Ponto de Análise 04 não foi encontrado na organização**. O Quadro 24 descreve as citações dos colaboradores referentes ao Ponto de Análise 04.

Quadro 24. Descrição do Ponto de Análise 04 na Organização B.

Ponto de Análise	Resultado
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software. *(Colaborador C) "a gente faz o DAST, que é um teste baseado em sites públicos que estavam expostos publicamente para ver o quanto aquilo estava exposto ou não. Mas é muito mais pensado na segurança e não exatamente na privacidade dos dados."* *(Colaborador D) "utilizamos o SonarQube, algumas outras soluções para pegar a entropia de código, de segurança, token, hardcode e tudo mais. Mas agora um scan propriamente procurando pela palavra CPF, e-mail, coisas assim, eu não me recordo."* *(Colaborador C) "isso ocorre de forma periódica. Então, a gente fez uma vez o teste agora que a gente desenvolveu, daqui a 6 meses o time vai falar para a gente: 'seria legal a gente passar de novo para garantir que continua tudo ok depois que a gente teve mais alterações na aplicação'."*	○

A alta gerência da organização concorda que as questões relacionadas a privacidade de dados pessoais são importantes ao produto final e a imagem da organização perante seus clientes. Um modo de fomentar a disseminação de conhecimento aos seus colaboradores, é a disponibilidade de cursos internos em sua plataforma. No entanto, é de autonomia de cada colaborador escolher e fazer os cursos disponíveis e, conforme mencionado, os colaboradores priorizam cursos relacionados às tecnologias utilizadas no desenvolvimento de novas funcionalidades do sistema aos cursos relacionados à privacidade de dados pessoais.

Em relação ao produto de software, há um colaborador responsável pela priorização das demandas que serão implementadas pelo time de desenvolvimento, considerando as estratégias de negócio da organização. Entretanto, apesar da alta demanda pelo produto de software, sem os requisitos mínimos de privacidade de dados pessoais e segurança da informação, o produto de software não é entregue.

Durante a fase de refinamento de requisitos são identificados os usuários que utilizarão o sistema. Em alguns casos, o time de produto realiza pesquisas de preferências junto aos clientes. Outra estratégia utilizada pela organização são os experimentos nos quais novas funcionalidades são liberadas para 5% (cinco porcento) dos usuários a fim de coletar métricas e verificar dados referentes a experiência do usuário, afetando diretamente o software que está sendo desenvolvido. Com isso, o **Ponto de Análise 05 foi encontrado parcialmente na organização**. O Quadro 25 exibe as citações dos colaboradores referentes ao Ponto de Análise 05.

Quadro 25. Descrição do Ponto de Análise 05 na Organização B.

Ponto de Análise	Resultado
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software. *(Colaborador C) "o principal motivo que a empresa considera [importante as questões relacionadas a privacidade de dados pessoais] é para se proteger, proteger o próprio negócio. Porque qualquer vazamento você vai gerar prejuízo para cliente, você vai gerar prejuízo para a sua própria imagem. Isso pode acabar com o próprio negócio."* *(Colaborador D) "se não houvesse a legislação, e eu via isso acontecer quando não havia legislação, também. Ainda assim a empresa se preocupa, porque um vazamento de dado crítico fere muito a imagem da empresa".*	◐

(Colaborador C) "existe muito material institucional sobre segurança da aplicação, segurança no desenvolvimento, não só na privacidade de dados. Eu diria que é um pouco mais amplo, isso sempre pensando no cliente." *(Colaborador C) "Existe muito material, mas é dada autonomia para que os engenheiros escolham os cursos que querem fazer."* *(Colaborador D) "[...] segurança é um ponto crítico que nenhum projeto pode pular. Então, se a área de segurança não deu uma ok naquilo ali, provavelmente aquilo não consegue seguir para a produção."* *(Colaborador C) "[...] talvez, o que é mais aceitável a se fazer é: 'talvez a gente não consiga fazer o que a gente acha que é o modelo ideal de segurança e privacidade agora, mas a gente vai colocar um outro mínimo e daqui a gente sai com um débito técnico para resolver, para aperfeiçoar o que a gente vai lançar em um segundo momento.'. Isso é o máximo que eu vejo de flexibilidade para isso acontecer."* *(Colaborador D) "O que acontece muito é simplificar o MVP para não precisar desse dado e lançar alguma coisa mais simples, porque fere a área de segurança também. Isso não consegue prosseguir dentro do fluxo."* *(Colaborador C) "Durante o refinamento essa é uma das principais perguntas que a gente faz para o nosso time de produto: 'Quais são os casos de uso?'. Com os casos de uso a gente consegue entender quais são os usuários que vão utilizar aquela feature."* *(Colaborador C) "Uma das possibilidades que tem é eles [o time de produto] fazerem alguma pesquisa de preferência com clientes. Mas o que a gente usa muito mais hoje é a questão de fazer experimentos. [...] é fazer, como se fosse, uma feature flag em produção, e aquela nova feature a gente manda só para 5% dos nossos usuários totais. Baseado nisso, a gente coleta métricas para falar assim: 'o cara utilizando essa nova feature, a gente aumentou em x% a nossa conversão', por exemplo."*	

D.2.3 Análise de Proposições

Para a Proposição 1 definiu-se quatro pontos de análise. O primeiro ponto de análise está relacionado a existência de processos sistematizados que visam integrar a privacidade de dados pessoais ao desenvolvimento ágil de software. Durante a análise verificou-se que a organização utiliza o modelo de processo Scrum no desenvolvimento de seus produtos. Porém, não são estabelecidas atividades sistematizadas que visam identificar problemas e propor soluções para questões relacionadas a privacidade de dados pessoais.

O segundo e terceiro pontos de análise referem-se à existência de especialistas em privacidade de dados pessoais na composição dos times de desenvolvimento e o conhecimento da área de privacidade de dados pessoais pela equipe técnica. Neste contexto, constatou-se que as equipes são formadas por profissionais com perfis

multidisciplinares, não havendo especialistas em áreas específicas. Os membros dos times devem ter diversas habilidades como designer, desenvolvedor *front* e *back-end*, testador, além do conhecimento de normas, leis e regulamentos para adequar o produto a legislação vigente.

O quarto e último ponto de análise diz respeito ao uso de ferramentas que auxiliam a integração da privacidade de dados pessoais ao desenvolvimento do produto de software. Neste ponto não foi constatado o uso de ferramentas voltadas a privacidade de dados pessoais. Sendo assim, a **Proposição 1 foi considerada verdadeira**. O Quadro 26 apresenta a análise da Proposição 1 na Organização B.

Quadro 26. Análise da Proposição 1 na Organização B.

Análise da Proposição	Resultado
Proposição 1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	○
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	○
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	◐
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	○

A Proposição 2 é representada apenas por um ponto de análise na qual se identificou que, apesar da preocupação em não priorizar requisitos funcionais em detrimento da privacidade de dados pessoais, a organização não fomenta a aquisição de conhecimento e atualizações de seus colaboradores no que diz respeito a este tema.

Durante as entrevistas, constatou-se que a organização dispõe de recursos para investimento em treinamento do corpo técnico, porém, há ausência de incentivo destes orçamentos para a área de privacidade de dados pessoais. Desse modo, a

Proposição 2 foi considerada parcialmente verdadeira. O Quadro 27 apresenta a análise da Proposição 1 na Organização B.

Quadro 27. Análise da Proposição 2 na Organização B.

Análise da Proposição	Resultado
Proposição 2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	◐
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	◐

D.3 Organização C

- **Atividades da organização:** Desenvolvimento de Hardware e Software.
- **Caracterização da Organização:** Capital Privado.
- **Número de Colaboradores:** +10.000.
- **Área de atendimento ao cliente:** Diversas áreas.

D.3.1 Perfis dos Colaboradores

Neste estudo entrevistou-se dois colaboradores da Organização C. Suas respectivas funções, experiências, tempo de organização e duração da entrevista são descritos no Quadro 28.

Quadro 28. Organização C - Perfis dos Colaboradores.

Organização C	Função/Cargo	Tempo de trabalho na Organização	Tempo de Experiência (desde a graduação)	Duração da Entrevista
Colaborador E	Engenheiro de Software Sênior	2 anos e 1 mês	12 anos	00:46:27
Colaborador F	Analista de Segurança da Informação	4 anos e 8 meses	15 anos	00:42:14

D.3.2 Descrição dos Pontos de Análise

A Organização C possui como principal atividade o desenvolvimento, tanto de hardware quanto de software, além de prestar assistência técnica aos seus clientes. Para o desenvolvimento e manutenção de software, a organização possui um processo bem definido baseado no Scrum e Kanban, com *sprints* de duas semanas, além dos ritos como, *sprint planning*, *daily meeting*, *sprint review* e *sprint retrospective*.

Devido à sobrecarga de responsabilidade do *Product Owner* (PO), que responde a alta gerência da organização pelos sistemas, instituiu-se dois novos papéis: *Product Manager* (PM) e *Cross Product Leader* (CPL). O primeiro é responsável por conhecer a regra de negócio da organização e manter contato direto com o departamento de Business, e o segundo, é responsável por criar histórias de usuário, definir tarefas e solicitar mudanças aos times de desenvolvimento. Entretanto, não há no processo de desenvolvimento de software da organização, uma atividade responsável pela identificação de problemas e soluções relacionados à privacidade de dados pessoais.

A fim de manter a privacidade de dados pessoais dos clientes, os colaboradores manipulam bases de dados contendo informações fictícias. Os dados reais do sistema são mantidos em bases criptografadas as quais são acessadas apenas por colaboradores específicos.

Anualmente os colaboradores analisam os campos da base de dados a fim de classificá-los quanto ao nível acesso, isso ocorre devido as possíveis vulnerabilidades geradas a partir das alterações realizadas na base de dados durante o ano. Nesta classificação, quando um campo é definido como restrito, o mesmo deve ser/estar criptografado. Ao fim deste processo, é gerado um relatório contendo uma descrição do campo, tipo de dado, classificação e se está ou não criptografo. Portanto, o **Ponto de Análise 01 foi encontrado parcialmente na organização**.

O Quadro 29 aborda as citações dos colaboradores da Organização C referente ao Ponto de Análise 01.

Quadro 29. Descrição do Ponto de Análise 01 na Organização C.

Ponto de Análise	Resultado
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software. *(Colaborador E) "Hoje, a gente usa o Azure DevOps, que é uma união do Scrum com o Quadro Kanban. Você vai ter umas histórias, para fazer, fazendo, review. Sprints de duas semanas."* *(Colaborador E) "[...] a gente faz [todos as cerimônias]: a daily, retrospective, planning e review."* *(Colaborador F) "[atividade] específica [para privacidade de dados], não."*	◐

(Colaborador E) "O Product Owner é o dono do aplicativo, e ela quem vai responder para um nível acima. Então, se chegar um CEO, vai conversar direto com ela. O Product Manager é a pessoa que vai conhecer a regra de negócio e tem que conversar com o business, por exemplo. E eu tenho o Cross Product Leader, que cuida mais de um aplicativo. É essa pessoa que vai criar change, que vai criar história, que vai dividir tasks e essas coisas assim." *(Colaborador F) "os dados que eu trabalho são todos fictícios, eu só tenho dados reais em produção. E são todos criptografados. Tudo o que eu mexo são dados irreais."* *(Colaborador F) "Uma vez por ano, vem um relatório grande onde a gente tem que analisar todos os campos das bases de dados. [...] Eu tenho que classificar entre 'restrito', 'público', 'interno', tinham umas cinco classificações. E, se fosse restrito ou alguma coisa assim, eu tinha que falar se estava criptografado ou não."* *(Colaborador E) "Tem a parte de segurança mesmo, que é no dia a dia, reuniões semanais. Onde é pego outros tipos de situações, mais de segurança do que privacidade de dados. Privacidade de dados é mais uma vez por ano esse relatório. [Nesse relatório é descrito] o que cada campo é, tipo de dado, o que é a informação que está ali, classificação dela, se ela está criptografada ou não, se ela é usada em ambiente de não produção."*	

Os times de desenvolvimento são formados por membros com habilidades multidisciplinares. Os conhecimentos mais requisitados aos colaboradores são de design e desenvolvimento, não sendo necessário a estes colaboradores um entendimento aprofundado em questões de privacidade de dados pessoais e segurança da informação.

Entretanto, há na organização uma equipe específica que possui a responsabilidade de receber os softwares desenvolvidos pelos times de desenvolvimento a fim de testá-los quanto a suas vulnerabilidades, tanto de segurança da informação quanto de privacidade de dados pessoais. Porém, os membros desta equipe não integram os times de desenvolvimento.

Como resultado, relatórios são gerados e repassados aos times de desenvolvimento para que eles solucionem os problemas encontrados. Para isso, o time de desenvolvimento pode consultar guias específicos para a vulnerabilidade encontrada ou questionar a equipe de teste sobre possíveis soluções para o problema identificado. Desta maneira, o **Ponto de Análise 02 não foi encontrado na organização**. O Quadro 30 destaca as citações dos colaboradores da Organização C referente ao Ponto de Análise 02.

Quadro 30. Descrição do Ponto de Análise 02 na Organização C.

Ponto de Análise	Resultado
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software. *(Colaborador E) "os times são subdivididos. Não tem espaço para ter uma pessoa só para isso (especialista em privacidade de dados pessoais). [...] São três desenvolvedores nos times."* *(Colaborador F) "O design e a implementação. E a parte que mais complica, a infra. A instalação do weblogic, a instalação de tudo, a atualização do Java, é tudo com a gente."* *(Colaborador F) "tem uma outra equipe que gera o relatório. Uma outra equipe separada, que eles chamam de DFS, que é uma equipe de segurança, essa equipe de dados mesmo e de privacidade que é só para isso."* *(Colaborador E) "eles [a equipe de privacidade de dados] tem muita coisa documentada, muito tutorial. Então 'você caiu na vulnerabilidade de privacidade 352', você abre lá: 'ah, é porque meu dado está como privado, mas não está criptografado'. Então, já tem aquilo, e se ainda for necessário eu falo com a pessoa."*	○

Apesar do time de desenvolvimento não ser composto por especialistas em áreas específicas, os integrantes do time devem submeter seus aplicativos contemplando requisitos não funcionais, como privacidade e segurança de dados, para homologação. Para isto, a organização disponibiliza diversos cursos aos seus colaboradores que devem ser realizados no momento da contratação do profissional.

Constatou-se também que anualmente a organização disponibiliza novos cursos e atualiza os existentes como iniciativa de incentivar seus colaboradores a manter-se atualizados. Por sua vez, estes profissionais devem cumprir uma carga horária mínima anual de cursos realizados.

Caso o colaborador sinta deficiência em uma determinada área e necessite realizar cursos externos, a organização disponibiliza recursos para este fim. Cada colaborador possui autonomia em escolher os cursos que melhor trará resultados a ele, incluindo o tema de privacidade de dados pessoais. Sendo assim, o **Ponto de Análise 03 foi encontrado na organização**. O Quadro 31 aborda as citações dos colaboradores da Organização C referente ao Ponto de Análise 03.

Quadro 31. Descrição do Ponto de Análise 03 na Organização C.

Ponto de Análise	Resultado
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização. *(Colaborador F) "quando você começa na [organização], você é obrigado a fazer os cursos."* *(Colaborador E) "somos obrigados a fazer os cursos, entre eles o de privacidade de dados. Todo ano troca [os cursos] e é obrigado a fazer. Eles [a alta gerência] obrigam com uma carga mínima de cursos por ano e com os requisitos implementados corretamente no sistema."* *(Colaborador F) "Se eu quiser, eu posso. Eu tenho um valor anual que eu posso escolher os cursos. Não necessariamente vai ser para essa área [privacidade de dados pessoais]. Eu posso escolher para o que eu quiser. Se eu achar que estou com deficiência nisso, eu posso optar por algum curso nisso."*	●

Identificou-se que uma preocupação da organização com questões relacionadas à segurança da informação. Nos últimos anos a organização está investimento na contratação de especialistas e ferramentas para se tornar referência neste quesito. No entanto, quando se trata especificamente de privacidade de dados pessoais, o time de desenvolvimento não dispõe de ferramentas que os auxiliam na detecção de possíveis vulnerabilidades.

Atualmente, a equipe de desenvolvimento faz uso de diretrizes internas na organização para detectar e solucionar problemas relacionados a privacidade de dados pessoais. Porém, este processo é inteiramente manual e o guia apenas auxilia os profissionais neste procedimento. Desse modo, o **Ponto de Análise 04 não foi encontrado na organização**. O Quadro 32 exibe as citações dos colaboradores da Organização C referente ao Ponto de Análise 04.

Quadro 32. Descrição do Ponto de Análise 04 na Organização C.

Ponto de Análise	Resultado
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software. *(Colaborador F) "tem esse relatório uma vez por ano, que é uma ferramenta, mas não dá para colocar a palavra ágil junto, porque é uma vez por ano."*	○

(Colaborador E) "se a gente criar um campo novo, a gente mesmo tem que ter a noção do que a gente está guardando naquele campo e se deve ser criptografado ou não". *(Colaborador E) "é mais um guia. Eu como dev que digo se o campo é ou não importante. Não tem uma ferramenta em si que vai adivinhar o nome do campo. [...] Por isso que é uma análise manual mesmo feito com business."*	

A preocupação da alta gerência da organização se concentra em manter-se em conformidade com as legislações vigentes. Com isso, os requisitos funcionais não são priorizados em detrimento a privacidade de dados pessoais. Portanto, os times de desenvolvimento de software devem seguir as políticas estabelecidas a respeitar questões relacionadas a este tema. Nos casos em que um produto não atinge requisitos mínimos de privacidade, a equipe responsável pelo sistema deverá solucionar o problema com prioridade máxima.

Constatou-se que há na organização uma política de identificação dos usuários da aplicação. Estes são envolvidos diretamente no processo de desenvolvimento do software, e as opiniões fornecidas por eles são consideradas a fim de realizar modificações no sistema, se necessário. Com isso, o **Ponto de Análise 05 não foi encontrado na organização**. O Quadro 33 aborda as citações dos colaboradores da Organização C referente ao Ponto de Análise 05.

Quadro 33. Descrição do Ponto de Análise 05 na Organização C.

Ponto de Análise	Resultado
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software. *(Colaborador E) "O que a equipe que cuida de dados pessoais fala, está falado. Se o seu sistema não atender isso até a data x, você entra em uma lista vermelha e é prioridade zero".* *(Colaborador E) "[...] a privacidade é mais importante do que código, é mais importante do que outra funcionalidade."* *(Colaborador F) "os testes passam pelos usuários. Se ele não der 'ok', não vai para frente. Quase toda história passa pelo usuário, só se eu determinar que não precisa. Mas se for algo que envolve business, que envolve regra de negócio, todas [histórias] passam por eles."*	

D.3.3 Análise de Proposições

Para a Proposição 1 definiu-se quatro pontos de análise. O primeiro ponto de análise está relacionado a existência de processos sistematizados que visam integrar a privacidade de dados pessoais ao desenvolvimento ágil de software. Durante a análise verificou-se que a organização utiliza o modelo Scrum e Kanban como processos de desenvolvimento ágil. Constatou-se que são realizadas as reuniões estabelecidas pelo Scrum e que, devido a responsabilidade alta demanda e excesso de responsabilidade do *Product Owner* (PO), um novo papel foi criado, denominado *Cross Product Leader* (CPL), este responsável pela definição de tarefas, criação de histórias de usuário e solicitação de alterações no produto. Entretanto, não se constatou no modelo de processo da organização a integração de atividades relacionadas a privacidade de dados pessoais.

O segundo pontos de análise busca identificar se há especialistas em privacidade de dados pessoais na composição dos times ágeis. Verificou-se que não há profissionais especialistas nos times de desenvolvimento de software. As equipes são formadas por membros com perfis multidisciplinares que devem ter conhecimento em privacidade de dados pessoais e segurança da informação.

No entanto, há na organização uma equipe especializada em problemas, tanto de segurança quanto de privacidade de dados pessoais, conforme verificado pelo terceiro ponto de análise. Esta equipe possui a responsabilidade de realizar testes a fim de encontrar vulnerabilidades. Porém, uma vez as encontradas, é dever do time de desenvolvimento saná-las.

Por fim, o quarto ponto de análise visa encontrar o uso de ferramentas que auxiliam os profissionais da organização na integração de privacidade de dados pessoais ao desenvolvimento de software. Verificou-se que os processos para identificar e solucionar problemas relacionados à privacidade de dados ocorrem de maneira totalmente manual. Desse modo, a **Proposição 1 foi considerada verdadeira**. O Quadro 34 apresenta a análise da Proposição 1 na Organização C.

Quadro 34. Análise da Proposição 1 na Organização C.

Análise da Proposição	Resultado
Proposição 1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	◐
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	○
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	●
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	○

A Proposição 2 considerou-se apenas um ponto de análise, no qual não se constatou a existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante a implementação de software. Verificou-se que estar em conformidade com a legislação é prioridade para a alta gerência da organização e que favorecer a entrega de software funcional em detrimento de requisitos não funcionais, como privacidade de dados, não ocorre na organização.

Corroborando com a Proposição 2, notou-se que os clientes são fundamentais no desenvolvimento do produto. As opiniões dos usuários são coletadas e implementadas como melhorias do produto final. Portanto, a **Proposição 2 foi considerada não verdadeira**. O Quadro 35 exibe a análise da Proposição 2 na Organização C.

Quadro 35. Análise da Proposição 2 na Organização C.

Análise da Proposição	Resultado
Proposição 2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	○
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	○

D.4 Organização D

- **Atividades da organização:** Desenvolvimento de Software.
- **Caracterização da Organização:** Sociedade Anônima.
- **Número de Colaboradores:** 100 – 999.
- **Área de atendimento ao cliente:** Diversas áreas.

D.4.1 Perfis dos Colaboradores

Neste estudo entrevistou-se dois colaboradores da Organização D. Suas respectivas funções, experiências, tempo de organização e duração da entrevista são descritos no Quadro 36.

Quadro 36. Organização D - Perfis dos Colaboradores.

Organização D	Função/Cargo	Tempo de trabalho na Organização	Tempo de Experiência (desde a graduação)	Duração da Entrevista
Colaborador G	Líder Técnico	14 anos e 10 meses	23 anos	00:50:37
Colaborador H	Coordenador de Qualidade de Software	16 anos e 1 mês	17 anos	00:45:24

D.4.2 Descrição dos Pontos de Análise

A Organização D tem como atividade principal o desenvolvimento de software, certificada pela ISO 9001:2015, e atende aproximadamente 2.000 (dois mil) clientes de diversos ramos, como governamental, farmacêutico, educação, manufatura, entre outros.

Tanto para o desenvolvimento quanto manutenção dos produtos, a organização possui um processo bem definido que une práticas do Scrum e do PMBOK. A gestão das tarefas ocorre por meio das cerimônias definidas no modelo Scrum, como *sprint planning*, *daily meeting* e *sprint review*, além de contar com *sprints* de duas semanas.

A gestão do projeto utiliza técnicas do PMBOK em que o projeto necessita estar com um escopo bem definido, pré-aprovado pela alta gerência e com um prazo estabelecido de entrega. Entretanto, não há uma atividade no processo de desenvolvimento que integre questões relacionadas à privacidade de dados pessoais, apenas uma política que auxilia o time de desenvolvimento em questões de segurança da informação, uma vez que os dados mentidos pela organização precisam estar em conformidade legal. Dessa maneira, o **Ponto de Análise 01 não foi encontrado na organização**. O Quadro 37 aborda as citações dos colaboradores da Organização D referente ao Ponto de Análise 01.

Quadro 37. Descrição do Ponto de Análise 01 na Organização D.

Ponto de Análise	Resultado
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software. *(Colaborador G) "A organização possui sim um processo bem estabelecido, um nível de maturidade já de mais de 10 anos para o desenvolvimento de software. [...] existe um processo tanto para a manutenção de software, como evolução, como um processo para correção. Esses processos são homologados e estão certificados pela ISO 9001"* . *(Colaborador G) "[...] é um processo híbrido que usa práticas do Scrum e práticas do PMBOK. [...] Por exemplo, práticas do Scrum tem as sprints, as reuniões diárias, [...] as cerimônias de daily, de planejamento, de planning, [...] tem os sprints que são definidos de duas semanas. [...] retrospectiva a gente não usa, isso é opcional. [...] a gestão da tarefa em si, a dinâmica pode ser o Scrum, mas a gestão do projeto em si não é ágil. Ele acaba sendo muito mais com ideias de PMBOK, onde você tem um escopo bem definido, pré-aprovado e você tem um prazo definido para a entrega."* *(Colaborador G) "[...] diretamente com o processo de desenvolvimento não há [há uma integração da privacidade de dados nos processos ágeis]."* *(Colaborador G) "existe uma política [de privacidade de dados], porém não existe um processo definido. Também não é integrado isso [a política de privacidade] ao processo de desenvolvimento."* *(Colaborador G) "ouvi falar [dos fundamentos do Privacy by Design], [...] mas, não. Neste momento a gente não usa deste framework."* *(Colaborador H) "ouvi falar [sobre Privacy by Design], mas muito por cima. Também não me aprofundei. Então, eu diria, praticamente zero."*	○

Os times de desenvolvimento são formados por quatro a oito colaboradores que assumem papéis de *product owner*, desenvolvedores e analistas da qualidade.

Constatou-se que profissionais específicos, como designers e administradores de banco de dados, compõem equipes separadas. Entretanto, a organização não possui especialistas em privacidade de dados, tampouco uma iniciativa para alocar profissionais com este perfil nas equipes de desenvolvimento, pois a organização terceiriza assuntos relacionados à privacidade de dados pessoais. Sendo assim, o **Ponto de Análise 02 não foi encontrado na organização**. O Quadro 38 destaca as citações dos colaboradores da Organização D referente ao Ponto de Análise 02.

Quadro 38. Descrição do Ponto de Análise 02 na Organização D.

Ponto de Análise	Resultado
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software. *(Colaborador G) "é uma equipe multidisciplinar, pois existe product owners, testers e desenvolvedores. [...] a quantidade varia, pode ter mais de um tester, mais de um product owner, depende do produto, depende do time. Mas os times variam entre, de quatro a oito, dez colaboradores."* *(Colaborador G) "As equipes de UX são separadas, isso é uma prática mais particular da empresa. As equipes de cloud são separadas e as equipes de dados também são separadas."* *(Colaborador G) "[os times] não [incorporam especialistas em privacidade de dados]. Porque como a gente tem isso terceirizado acaba ficando em um âmbito mais de DevOps e diretoria."* *(Colaborador G) "Não tem nem previsão [para haver uma iniciativa de alocação de profissionais especialistas em privacidade de dados pessoais]."*	○

Constatou-se que a organização dispõe de diferentes produtos os quais possuem suas particularidades quanto aos requisitos de privacidade de dados pessoais. Sendo assim, há uma organização terceirizada que realiza a atividade de verificar se estes produtos estão em conformidade com a legislação vigente. Por este motivo, não há um conhecimento aprofundado do corpo técnico da organização em privacidade de dados pessoais, além de não haver uma iniciativa para formar especialistas na área, visto que a organização não tem o objetivo de internalizar para si esta função.

Conforme relatado pelos entrevistados, há uma plataforma que possui cursos dos mais variados conteúdos, inclusive de privacidade de dados pessoais. Esta

plataforma visa proporcional aos colaboradores uma maneira de mantê-los atualizados e contribuir com o seu crescimento profissional. No entanto, são cursos básicos que não possuem o objetivo de formar especialistas nos conteúdos disponíveis.

Por outro lado, a organização disponibiliza recursos aos colaboradores que necessitem realizar cursos específicos. Sendo de responsabilidade e iniciativa do próprio colaborador solicitar. Desse modo, o **Ponto de Análise 03 não foi encontrado na organização**. O Quadro 39 aborda as citações dos colaboradores da Organização D referente ao Ponto de Análise 03.

Quadro 39. Descrição do Ponto de Análise 03 na Organização D.

Ponto de Análise	Resultado
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização. *(Colaborador G) "há treinamentos de boas práticas, porém não especificamente em privacidade de dados."* *(Colaborador G) "os treinamentos acabam sendo muito mais direcionados à pratica que a gente vai adotar ou a nossa necessidade. Então o que acaba não fazendo parte, muitas vezes isso não é divulgado ou fica a cargo de cada um procurar mais informações por interesse próprio."* *(Colaborador H) "o material é bem sucinto e não traz informação a nível de formar alguém. A informação é bem rasa. [...] Também o objetivo dele não é formar especialista, é só trazer um pouquinho de conhecimento."* *(Colaborador G) "não há iniciativa. Por exemplo, para promover um grupo para que virem [especialistas em privacidade de dados], não há iniciativa."* *(Colaborador G) "a gente investe, contrata consultores externos, contrata treinamentos para desenvolvimento ágil, [...] mas para privacidade, não."* *(Colaborador H) "tem que partir do colaborador. Sentiu necessidade, levanta a mão e vai cair o dinheiro lá para que o treinamento seja realizado. [...] Não tem ninguém olhando e [dizendo:] 'você precisa se desenvolver nesse requisito!'."*	○

A organização possui preocupação com a identificação de vulnerabilidade de codificação. Para isto, é utilizada a ferramenta Sonar que realiza análise estática do código-fonte para identificar comandos depreciados, criptografias básicas, entre outras vulnerabilidades. Porém, não se constatou o uso de ferramentas específicas a privacidade e proteção de dados pessoais. Com isso, o **Ponto de Análise 04 não foi**

encontrado na organização. O Quadro 40 aborda as citações dos colaboradores da Organização D referente ao Ponto de Análise 04.

Quadro 40. Descrição do Ponto de Análise 04 na Organização D.

Ponto de Análise	Resultado
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software. *(Colaborador G) "não especificamente [para privacidade de dados pessoais]. A única seria o Sonar, que só vê alguns níveis de vulnerabilidade."* *(Colaborador H) "para a segurança [da informação] a gente tem. Ou melhor, a gente tem até um processo um pouquinho melhor do que de proteção [de dados]. Para a proteção [de dados], não tem."*	

Apesar de não haver um interesse da alta gerência da organização em fomentar a contratação e formação de profissionais especializados em privacidade de dados pessoais, os diretores compreendem a necessidade e importância de contemplar requisitos de privacidade em seus produtos a fim de estar em conformidade com a LGPD. Isto é traduzido em investimentos na contratação de organizações terceiras que, por sua vez, possuem a responsabilidade de identificar e solucionar problemas relacionados a privacidade de dados.

Constatou-se que em cada produto são realizadas análises de riscos que visam identificar e classificar possíveis problemas relacionados aos requisitos não funcionais, como por exemplo, privacidade de dados. Caso existam problemas que contrariem a LGPD, o sistema não é disponibilizado aos clientes.

Devido à organização possuir seus produtos consolidados no mercado, os usuários de suas aplicações estão bem definidos. Porém, em produtos novos os usuários são consultados a fim de elicitar suas reais necessidades que poderão ser consideradas no momento do desenvolvimento dos sistemas. Entretanto, conforme relatados pelos entrevistados, esta é uma prática de responsabilidade e iniciativa do *Product Owner* de cada time e não há uma etapa no processo definida para este fim. Portanto, o **Ponto de Análise 05 foi encontrado na organização**. O Quadro 41 aborda as citações dos colaboradores da Organização D referente ao Ponto de Análise 05.

Quadro 41. Descrição do Ponto de Análise 05 na Organização D.

Ponto de Análise	Resultado
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software. *(Colaborador G) "Dado pelo investimento que tem nesta área a partir de uma empresa terceira e o custo que isso gera para a empresa. Não é um custo barato. Muito pelo contrário. A contratação de mais de uma empresa, a validação. Então, há sim um interesse muito grande da empresa. O que ela não tem é o interesse em trazer esse know how internamente."* *(Colaborador H) "A posição da direção de que é necessário e de que é prioritário, inclusive. Muito mais ligado a questão da lei e da penalidade, porque a multa é bem alta, do que exatamente a questão de gerar requisitos [de privacidade de dados]."* *(Colaborador H) "Se no escopo for identificado algum gap em relação à privacidade de dados, ele [sistema] não é liberado. [...] Nem para proteção de dados, nem para segurança [de dados]"* *(Colaborador G) "existe sim, mas isso como é um produto já institucionalizado há mais de quinze anos, então isso normalmente acaba sendo uma prática muito em produtos novos."* *(Colaborador H) "A direção hoje ela não bloqueia [a iniciativa de consultar os clientes], mas ela não incentiva. Então o PO quando está desenvolvendo um requisito novo, ele vai lá, chama um [cliente], chama outro, mas por iniciativa [própria], não por estar dentro de um processo."*	

D.4.3 Análise de Proposições

Há quatro pontos de análises relacionados a Proposição 1. O primeiro ponto de análise visa identificar na organização a existência de processos sistematizados que integram a privacidade de dados pessoais ao desenvolvimento ágil de software. Neste contexto, verificou-se que a organização utiliza práticas dos modelos Scrum e PMBOK nos desenvolvimentos de seus projetos. Porém, não foi constatado neste modelo atividades relacionadas a identificação e resolução de problemas de privacidade e proteção de dados pessoais.

O segundo ponto de análise tem como objetivo identificar especialistas em privacidade de dados pessoais na composição dos times de desenvolvimento da organização. Verificou-se que os números de colaboradores que integram as equipes de desenvolvimento são variados. Entretanto, os papéis são *Product Owner*, desenvolvedores e analistas da qualidade. Não há especialistas em privacidade de

dados pessoais na formação das *squads*, pois há uma organização terceirizada que possui a responsabilidade de identificar e documentar inconformidades legais dos produtos de software.

Sendo assim, não se identificou na organização uma equipe técnica com conhecimento aprofundado em privacidade de dados pessoais, tampouco ferramentas capazes de auxiliar na integração da privacidade de dados ao desenvolvimento de software, objetos investigados nos Pontos de Análises 03 e 04. Desse modo, a **Proposição 1 foi considerada verdadeira**. O Quadro 42 apresenta a análise da Proposição 1 na Organização D.

Quadro 42. Análise da Proposição 1 na Organização D.

Análise da Proposição	Resultado
Proposição 1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	○
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	○
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	○
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	○

Para a Proposição 2, considerou-se apenas o Ponto de Análise 05, relacionado a existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento de software. Neste ponto de análise, verificou-se que há uma preocupação da alta gerência da organização em estar em conformidade com a LGPD. Por isso, há investimentos na contratação de organizações terceiras as quais possuem a responsabilidade de identificar e reportar os problemas relacionados à privacidade de dados pessoais. Entretanto, não há até o momento investimentos em formar colaboradores internos neste assunto. Portanto, a

Proposição 2 foi considerada verdadeira. O Quadro 43 exibe a análise da Proposição 2 na Organização D.

Quadro 43. Análise da Proposição 2 na Organização D.

Análise da Proposição	Resultado
Proposição 2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	●
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	●

D.5 Organização E

- **Atividades da organização:** Serviços financeiros.
- **Caracterização da Organização:** Sociedade Anônima.
- **Número de Colaboradores:** 100 – 999.
- **Área de atendimento ao cliente:** Diversas áreas.

D.5.1 Perfis dos Colaboradores

Neste estudo entrevistou-se dois colaboradores da Organização E. Suas respectivas funções, experiências, tempo de organização e duração da entrevista são descritos no Quadro 44.

Quadro 44. Organização E - Perfis dos Colaboradores.

Organização E	Função/Cargo	Tempo de trabalho na Organização	Tempo de Experiência (desde a graduação)	Duração da Entrevista
Colaborador I	Arquiteto de Soluções	3 anos e 6 meses	22 anos	00:51:15
Colaborador J	Analista Sênior de Segurança da Informação	2 anos e 11 meses	18 anos	00:54:48

D.5.2 Descrição dos Pontos de Análise

A Organização E é uma organização do setor financeiro que atua principalmente no fornecimento de crédito consignado, investimentos e seguros aos seus clientes. Para melhor comodidade em atendê-los, possui um departamento específico no desenvolvimento de soluções digitais que permitem a contratação online de seus serviços.

Para o desenvolvimento e manutenção de seus sistemas, a Organização E conta com 16 times ágeis que utilizam o modelo Scrum ou Kanban no gerenciamento de seus projetos, dependendo da atuação de cada um. As *sprint* tem duração de duas

semanas e todas as cerimônias do Scrum são respeitadas, como por exemplo, *Sprint Planning*, *Daily Meeting*, *Sprint Review Meeting* e *Sprint Retrospective*. Entretanto, não há uma atividade integrada ao processo de desenvolvimento ágil que seja responsável pela identificação e correção de requisitos relacionados a privacidade de dados pessoais.

A verificação de conformidade legal ocorre após o time de desenvolvimento entregar uma funcionalidade, e é realizada por uma equipe constituída por dois colaboradores e uma consultoria contratada pela organização. Devido a limitação do número de colaboradores nesta equipe, há uma sobrecarga de trabalho impossibilitando atender a todos os times com a devida qualidade. Em alguns casos, o produto é colocado em produção sem o cuidado adequado com questões relacionadas à privacidade de dados pessoais. Com isso, o **Ponto de Análise 01 foi encontrado parcialmente na organização**. O Quadro 45 aborda as citações dos colaboradores da Organização E referente ao Ponto de Análise 01.

Quadro 45. Descrição do Ponto de Análise 01 na Organização E.

Ponto de Análise	Resultado
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software. *(Colaborador I) "[...] cada um dos times ágeis trabalha, ou com Scrum com duas semanas de sprint, ou com fluxo puxado com Kanban. Isso varia de time para time."* *(Colaborador I) "[...] planning, retrospective, tudo. [...] os times Scrum seguem todas as cerimônias, No kanban também nós temos um processo muito parecido com o do Scrum. Todo dia tem uma daily de 15 minutos por time. E também tem retrospectivas, mas ela não é tão constante como a do Scrum. Varia muito com a entrega de valor porque o kanban é um fluxo puxado."* *(Colaborador I) "Ela [consultoria] acontece basicamente no final do processo, quando nós já entregamos uma funcionalidade. [...] ela [consultoria] documenta aonde é a origem [do dado sensível], como acontece a transformação desses dados, como se dá a persistência da informação, quais são os possíveis usuários que utilizam aquela informação, quais os sistemas que utilizam aquela informação."* *(Colaborador J) "a gente está tentando colocar isso [verificação de requisitos de privacidade de dados pessoais] para ser antecipado, mas atualmente não é 100% que funciona assim."* *(Colaborador J) "Gera sim [uma sobrecarga de trabalho]. Até porque a gente precisa aumentar a equipe. Então é uma demanda que a gente precisa evoluir na questão de times para conseguir atender com qualidade."*	◐

(Colaborador I) "Eu conheço o Privacy by Design, que é o processo de você tentar identificar a privacidade no momento da concepção, mas hoje [a Organização E] não segue isso. A gente trabalha muito mais no final do processo do que no processo em si."	

Verificou-se que os times são formados por profissionais especialistas em áreas distintas. Cada time é composto por desenvolvedores *back-end*, *front-end*, analista de qualidade, líder de time e *product owner*. Além destes papéis, há o arquiteto, porém, este não compõe um time específico. Sua principal responsabilidade é dar suporte as equipes quando necessário.

No entanto, não há especialistas em privacidade de dados pessoais na composição dos times de desenvolvimento. Sendo de responsabilidade do *product owner* e do arquiteto a identificação dos requisitos funcionais e não funcionais, como por exemplo, privacidade de dados e segurança da informação. Além disso, constatou-se que atualmente não há uma iniciativa da organização para alocar especialistas de dados pessoais na formação dos times ágeis de desenvolvimento de software. Desse modo, o **Ponto de Análise 02 não foi encontrado na organização**. O Quadro 46 aborda as citações dos colaboradores da Organização E referente ao Ponto de Análise 02.

Quadro 46. Descrição do Ponto de Análise 02 na Organização E.

Ponto de Análise	Resultado
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software. *(Colaborador I) "[os times] são compostos de desenvolvedores front-end e back-end, [...] mais um QA [Quality Analyst], mais um team leader, mais um PO."* *(Colaborador I) "[...] os times não tem dentro de si um especialista em LGPD ou alguém especialista em privacidade. Muitas vezes esse papel fica distribuído com o próprio PO ou com o arquiteto em si."* *(Colaborador I) "cada um [membro do time de desenvolvimento] tem a sua especialidade, mas nenhum deles acabada trabalhando com privacidade ou segurança especificamente."* *(Colaborador I) "eu desconheço [a iniciativa da organização para alocar especialistas em privacidade nos times de desenvolvimento]. Eu acho que não tem essa iniciativa."*	

Apesar da organização contar com uma consultoria e um departamento jurídico, é de responsabilidade do time de desenvolvimento implementar os requisitos de privacidade de dados e segurança da informação em seus produtos. Para prover esse conhecimento ao colaborador, a organização disponibiliza cursos em diversas áreas por meio de uma plataforma digital, sendo de responsabilidade do colaborador realiza-los semestralmente. Além disso, tanto o departamento jurídico quanto o especialista em privacidade de dados pessoais da organização estão em constante comunicação com todos os times de desenvolvimento, podendo estes solicitar reuniões ou consultorias internas a fim de sanar dúvidas relacionadas à LGPD.

Conforme relatado pelos entrevistados, os cursos atendem todos os colaboradores da organização, sendo assim, estes cursos possuem um conteúdo básico dos assuntos abordados e não visam formar profissionais especialistas em determinadas áreas.

Entretanto, como o time de desenvolvimento possui a responsabilidade de entregar valor, muitas vezes as questões de privacidade de dados e segurança da informação são negligenciadas. Neste cenário, é de obrigação dos arquitetos e product owners se preocuparem com o ciclo de vida dos dados. Dessa maneira, o **Ponto de Análise 03 foi encontrado parcialmente na organização**. O Quadro 47 aborda as citações dos colaboradores da Organização E referente ao Ponto de Análise 03.

Quadro 47. Descrição do Ponto de Análise 03 na Organização E.

Ponto de Análise	Resultado
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização. *(Colaborador I) "existe uma plataforma [da organização] que é uma plataforma para conteúdos, cursos obrigatórios sobre segurança, privacidade, e todos os funcionários [da organização] tem que passar por esses treinamentos."* *(Colaborador J) "existe uma plataforma de treinamento para isso, mas é para uma coisa muito mais básica, não detalhando conceitos avançados ou se o colaborador deve atuar com governança dos dados ou com privacidade. É mais aqueles cursos introdutórios: O que é LGPD. O que é um dado sensível. Mas não dizendo como tratar a informação."* *(Colaborador J) "Dependendo do time, eles solicitam mais informações. Eles marcam reuniões comigo ou com meu colega de trabalho para entender qual é a interpretação da lei diante de um fato que eles querem alterar um processo atual. Então a gente acaba fazendo essa consultoria interna também."*	

(Colaborador I) "Hoje esse papel de entendimento dos processos, dos dados, da estrutura de como funcionam as coisas em relação aos dados e privacidade, ela fica muito difundida entre o PO e o arquiteto. Às vezes o dev team, os desenvolvedores e o time de qualidade acabam nem percebendo que isso acontece ou, às vezes, nem é envolvido nisso porque eles trabalham no aspecto de, muito mais, de fazer a entrega do valor."	

A base de dados da Organização E está atualmente hospedada na plataforma Microsoft Azure[39], a qual fornece configurações padrão de privacidade de dados, tanto para a LGPD quanto para o GDPR. Com isso, é possível definir quais dados são sensíveis e quais usuários possuem permissões de acesso a uma determinada informação.

Para o acesso às bases de dados, a organização utiliza um *middleware* chamado Securiti.AI[40], que é responsável pela identificação dos dados pessoais do titular, além de prover atendimento ao mesmo, possibilitando-o ter conhecimento de quais dados pessoais a organização armazena, além de executar ações como atualizações e exclusões de seus dados. Portanto, o **Ponto de Análise 04 foi encontrado na organização**. O Quadro 48 exibe as citações dos colaboradores da Organização E referente ao Ponto de Análise 04.

Quadro 48. Descrição do Ponto de Análise 04 na Organização E.

Ponto de Análise	Resultado
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software. *(Colaborador I) "Como todo o nosso banco de dados é na cloud, no Microsoft Azure. Os bancos de dados na Azure têm uma configuração padrão que funciona para a LGPD e para o GDPR, que você diz, você consegue dizer, daquela estrutura de dados que está governando dentro do ambiente cloud, quais devem ser sensíveis e quais não devem. E, a partir disto, você define quem deve ou não visualizar a informação."* *(Colaborador J) "nós temos uma ferramenta que conecta em todas as bases de dados. A gente faz uma leitura para identificar onde tem dado pessoal. Esse sistema também atua como um atendimento ao titular. Se o titular exerce seu direito à privacidade, essa ferramenta está integrada para poder já trazer esse dado direto no sistema. [...] Adicionalmente também nessa ferramenta estão os processos, que seriam os tratamentos de dados formalizados que estão vinculados a cada um dos bancos. De forma rápida consegue já trazer e apresentar para o titular um acesso, uma alteração, uma exclusão e aonde tem o dado dele aqui dentro."*	

[39] Site Microsoft Azure: https://azure.microsoft.com/
[40] Site Securiti.AI: https://securiti.ai/

(Colaborador I) "[as ferramentas são utilizadas] em todas as fases. Desenvolvimento, homologação e produção."	

A alta gerência compreende que a privacidade de dados pessoais agrega valor ao produto de software, fato comprovado pela contratação de consultorias e profissionais especializados para auxiliar na adequação à LGPD. Porém, não há, atualmente, uma política que incentive a integração da privacidade de dados ao desenvolvimento ágil de software, sendo a mesma tratada em uma etapa tardia do desenvolvimento do software.

Conforme mencionado em pontos de análises anteriores, o time de desenvolvimento possui o foco na entrega de valor, o que, em alguns casos, significa conceber um software funcional em um curto espaço de tempo em detrimento aos requisitos de privacidade de dados pessoais. Para isto, os sistemas desenvolvidos são submetidos à Subcomissão de Riscos e Governança que avalia a possibilidade de homologar uma funcionalidade mesmo não estando em conformidade legal.

Por outro lado, os usuários são consultados para auxiliar no desenvolvimento do sistema. Para esta atividade há profissionais especializados em experiência dos usuários que realizam pesquisas de campo a fim de verificar a percepção dos indivíduos em relação ao sistema as quais podem resultar em alterações no software. No entanto, esta atividade está voltada a requisitos de interface do sistema e usabilidade e não privacidade de dados pessoais. Sendo assim, o **Ponto de Análise 05 foi encontrado na organização**. O Quadro 49 destaca as citações dos colaboradores da Organização E referente ao Ponto de Análise 05.

Quadro 49. Descrição do Ponto de Análise 05 na Organização E.

Ponto de Análise	Resultado
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software. *(Colaborador I) "hoje não há [integração da privacidade de dados ao desenvolvimento de software]. O que existe é basicamente em relação a agilidade dentro [da organização] é a entrega de valor constante. A partir de uma especificação, identificado um valor de negócio e entregue. À medida que isso é entregue, aí sim que é entendido como integrar esses dados, essa funcionalidade junto a proteção de dados."*	

(Colaborador I) "[...] as vezes acabada entrando em produção uma coisa que a gente precisa ir lá em produção, rever e até apontar: 'opa, nós estamos com um risco aqui para ser avaliado e decidido na organização.'" *(Colaborador I) "[...] nós temos um comitê de gestão de risco. Então depende muito do que acontece. Vou dizer assim para você, se analisado pelo PO ou pelo arquiteto que: 'vamos deixar de ganhar dinheiro em relação a funcionalidade em relação a privacidade', isso é submetido a um comitê de gestão de risco. Esse comitê verifica se é um risco alto, baixo, médio, e verifica se faz sentido eu postergar ou não."* *(Colaborador J) "[...] existe a Subcomissão de Riscos e Governança, aonde é essa decisão de aprovar um risco, assumi-lo ou aprovar o plano de mitigação de exceção, ela é aprovada nessa gestão de riscos, nessa subcomissão de gestão de riscos."* *(Colaborador I) "nós temos pesquisas de UX. Nossa equipe de usabilidade sempre faz protótipos de usabilidades não funcionais e nossos UX tem alguns que são especialistas em pesquisas de campo. Eles acabam contatando os clientes para fazerem essas pesquisas. Então eles acabam levantando a interação do usuário em relação ao sistema, mas eu nunca percebi em relação à privacidade."*	

D.5.3 Análise de Proposições

Para a Proposição 1 estabeleceu-se quatro pontos de análise. O primeiro ponto de análise está relacionado a existência de processos sistematizados que visam integrar a privacidade de dados pessoais ao desenvolvimento ágil de software. Durante a análise verificou-se que a organização utiliza o modelo Scrum e Kanban como processos de desenvolvimento ágil de software. Constatou-se que são realizadas todas as cerimônias estabelecidas pelo Scrum e que, mesmo quando o time utiliza o Kanban, há também alguns ritos a serem seguidos. No entanto, a preocupação com questões de privacidade de dados pessoais ocorre de maneira tardia após a entrega de valor pelo time de desenvolvimento. Ou seja, estes requisitos não funcionais não são integrados ao processo ágil de desenvolvimento.

O segundo ponto de análise diz respeito a verificação da existência de especialistas em privacidade de dados pessoais nos times de desenvolvimento. Conforme analisado, a equipe de desenvolvimento é formada por especialistas em diversas áreas, como desenvolvedor *back-end*, *front-ent*, analista de qualidade e *product owner*. Entretanto, não há um especialista em privacidade de dados pessoais compondo o time de desenvolvimento. Este profissional existe na organização, mas atua separadamente como um consultor técnico a todos os times da organização.

Em relação ao terceiro ponto de análise, existência de conhecimento da área de privacidade de dados pessoais pela equipe técnica da organização. Constatou-se

que há uma equipe formada por dois profissionais especialistas em privacidade de dados, os quais, juntamente com o departamento jurídico, possuem a responsabilidade de auditar os produtos desenvolvidos a fim de verificar se estão em conformidade com a LGPD. Além disso, há uma plataforma na qual os colaboradores da organização são estimulados a realizarem cursos de diversas áreas, entre elas, privacidade de dados pessoais. Ressalta-se que estes cursos possuem conteúdos introdutórios e não visam formar especialistas nas respectivas áreas.

Por fim, o quarto ponto de análise tem o intuito de verificar a existência de ferramentas que auxiliam na integração da privacidade de dados pessoais nas atividades de desenvolvimento de software. Constatou-se que a organização utiliza sua base de dados na nuvem por meio da ferramenta Microsoft Azure e, para acessar os dados, a organização utiliza a ferramenta Securiti.AI, que realiza toda a comunicação e controle de acesso às informações contidas no banco de dados. Dessa maneira, a **Proposição 1 foi considerada verdadeira**. O Quadro 50 apresenta a análise da Proposição 1 na Organização E.

Quadro 50. Análise da Proposição 1 na Organização E.

Análise da Proposição	Resultado
Proposição 1: As organizações de desenvolvimento ágil de software não integram os princípios do PbD em seus processos de desenvolvimento de forma sistematizada.	●
Ponto de Análise 01: Existência de processos sistematizados que integram a privacidade de dados pessoais no desenvolvimento ágil de software.	◐
Ponto de Análise 02: Existência de especialistas em privacidade de dados pessoais na composição dos times no contexto ágil de desenvolvimento de software.	○
Ponto de Análise 03: Existência de conhecimento na área de privacidade de dados pessoais pela equipe técnica da organização.	◐
Ponto de Análise 04: Existência de ferramentas que auxiliam na integração da privacidade de dados pessoais ao desenvolvimento de produtos de software.	●

A Proposição 2 considerou-se apenas um ponto de análise, no qual constatou-se que, apesar da alta gerência ter conhecimento da importância de contemplar

questões relacionadas a privacidade de dados pessoais em seus produtos, não há uma política que visa integrar a privacidade de dados ao processo de software. Atualmente, na organização, há apenas dois especialistas em privacidade de dados que prestam assessoria aos dezesseis times de desenvolvimento, o que gera uma alta demanda destes profissionais o que resulta em, alguns casos, priorizar a entrega dos produtos no prazo estabelecido em detrimento aos requisitos de privacidade de dados pessoais.

Verificou-se que os usuários são constantemente consultados para validar os produtos que estão em desenvolvimento. Porém, estas atividades focam em requisitos de usabilidade e experiência do usuário. Não sendo abordados os requisitos de privacidade de dados. Sendo assim, a **Proposição 2 foi considerada verdadeira**. O Quadro 51 aborda a análise da Proposição 2 na Organização E.

Quadro 51. Análise da Proposição 2 na Organização E.

Análise da Proposição	Resultado
Proposição 2: As organizações de desenvolvimento de software enfrentam dificuldades em reformular seus processos em busca da conformidade com as leis e regulamentos.	●
Ponto de Análise 05: Existência de fatores que dificultam a priorização das questões de privacidade de dados pessoais durante o desenvolvimento ágil de software.	●

APÊNDICE E – MAPEAMENTO REALIZADO PELOS PARTICIPANTES

Cada participante realizou individualmente o mapeamento dos 72 Padrões de Privacidade com os Princípios do *Privacy by Design (PbD)*. Os Quadros 52, 53 e 54 apresentam o mapeamento realizado, respectivamente, pelos Participante A, B e C. As linhas que apresentam o caractere (●) indicam que o padrão de privacidade em questão contempla o princípio do PbD respectivo à coluna. Por outro lado, sua ausência indica a não relação.

Quadro 52. Mapeamento dos Padrões de Privacidade e Princípios do PbD – Participante A

Participante A								
Estratégia de Hoepman	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Abstract	Location Granularity	●	●	●				●
Control	Decoupling [content] and location information visibility	●		●			●	●
Control	Active broadcast of presence	●					●	●
Control	Buddy List				●			●
Control	Discouraging blanket strategies	●		●				●
Control	Enable/Disable Functions			●			●	●
Hide Control	Encryption with user-managed keys	●	●	●		●		
Control	Incentivized Participation	●	●					●
Inform Control	Informed Consent for Web-based Transactions						●	●
Control	Lawful Consent	●	●	●				●
Control	Masquerade					●	●	●
Control	Negotiation of Privacy Policy	●	●					●
Control	Outsourcing [with consent]	●	●				●	●
Control	Pay Back	●		●				●
Control	Obtaining Explicit Consent	●					●	●
Separate Control	Personal Data Store			●		●	●	●
Control	Private link		●	●				
Control	Reasonable Level of Control	●		●			●	●
Control	Reciprocity			●			●	●
Control	Selective access control		●	●				●
Control	Selective Disclosure	●	●	●				●
Control	Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context	●					●	●
Control	Single Point of Contact	●		●		●	●	●
Separate	User data confinement pattern	●		●				

Minimize Hide	Added-noise measurement obfuscation	●	●	●				●
Hide	Aggregation Gateway	●	●	●		●		
Hide	Trustworthy Privacy Plug-in		●			●		
Hide	Anonymity Set	●	●					
Hide Separate	Anonymous Reputation-based Blacklisting	●	●	●	●			
Hide	Onion Routing	●	●	●		●		
Hide	Pseudonymous Identity	●	●	●	●			
Hide	Pseudonymous Messaging	●		●		●		
Hide	Use of dummies		●	●				
Hide	Attribute Based Credentials	●	●					
Minimize	Protection against Tracking	●		●				●
Minimize	Strip Invisible Metadata	●		●	●		●	
Enforce	Federated Privacy Impact Assessment	●		●			●	
Enforce	Obligation Management	●		●			●	
Enforce	Sticky Policies	●		●			●	
Enforce	Identity Federation Do Not Track Pattern	●		●				
Inform	Abridged Terms and Conditions						●	●
Inform	Appropriate Privacy Icons						●	
Inform	Ambient Notice	●		●			●	●
Inform	Appropriate Privacy Feedback	●					●	●
Inform	Asynchronous notice						●	
Inform	Awareness Feed						●	●
Inform	Data Breach Notification Pattern			●			●	●
Inform	Privacy Aware Wording			●			●	
Inform	Dynamic Privacy Policy Display						●	●
Inform	Privacy icons						●	
Inform	Icons for Privacy Policies						●	
Inform	Layered Policy Design						●	
Inform	Privacy Labels							●
Inform	Privacy Policy Display						●	
Inform	Impactful Information and Feedback						●	●
Inform	Platform for Privacy Preferences			●				●
Inform	Policy Matching Display						●	●
Inform	Privacy-Aware Network Client						●	●
Inform	Increasing awareness of information aggregation						●	●
Inform	Informed Credential Selection						●	●
Inform	Informed Secure Passwords	●				●		●
Inform	Unusual Activities							●
Inform	Informed Implicit Consent						●	●
Inform	Minimal Information Asymmetry	●	●				●	●
Inform	Personal Data Table						●	●
Inform	Preventing mistakes or reducing their impact							●
Inform	Privacy Awareness Panel	●					●	

Inform	Privacy dashboard	●					●	
Inform	Privacy Color Coding						●	
Inform	Privacy Mirrors						●	●
Inform	Trust Evaluation of Services Sides							●
Inform	Who's Listening						●	●

Quadro 53. Mapeamento dos Padrões de Privacidade e Princípios do PbD – Participante B

Participante B								
Estratégia de Hoepman	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Abstract	Location Granularity	●	●	●				●
Control	Decoupling [content] and location information visibility	●	●	●				●
Control	Active broadcast of presence		●				●	●
Control	Buddy List				●		●	●
Control	Discouraging blanket strategies	●	●	●			●	●
Control	Enable/Disable Functions	●	●	●			●	●
Hide Control	Encryption with user-managed keys	●	●	●		●		●
Control	Incentivized Participation	●		●				●
Inform Control	Informed Consent for Web-based Transactions							●
Control	Lawful Consent	●		●			●	●
Control	Masquerade			●		●		●
Control	Negotiation of Privacy Policy	●	●					●
Control	Outsourcing [with consent]	●					●	
Control	Pay Back	●		●			●	●
Control	Obtaining Explicit Consent	●					●	
Separate Control	Personal Data Store		●	●			●	●
Control	Private link	●	●	●				
Control	Reasonable Level of Control	●		●				●
Control	Reciprocity		●	●			●	●
Control	Selective access control		●	●			●	●
Control	Selective Disclosure	●		●				●
Control	Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context	●						●
Control	Single Point of Contact	●		●		●		●
Separate	User data confinement pattern	●	●	●				
Minimize Hide	Added-noise measurement obfuscation	●	●	●				
Hide	Aggregation Gateway	●	●	●		●		
Hide	Trustworthy Privacy Plug-in			●		●	●	
Hide	Anonymity Set			●				
Hide Separate	Anonymous Reputation-based Blacklisting		●	●	●	●	●	

Hide	Onion Routing	●		●		●		
Hide	Pseudonymous Identity	●	●	●				
Hide	Pseudonymous Messaging			●		●	●	
Hide	Use of dummies		●	●				
Hide	Attribute Based Credentials	●	●					●
Minimize	Protection against Tracking	●	●	●				●
Minimize	Strip Invisible Metadata	●	●	●	●			
Inform	Abridged Terms and Conditions						●	
Inform	Appropriate Privacy Icons						●	
Inform	Ambient Notice	●	●	●				●
Inform	Appropriate Privacy Feedback						●	●
Inform	Asynchronous notice	●					●	●
Inform	Awareness Feed						●	●
Inform	Data Breach Notification Pattern						●	●
Inform	Privacy Aware Wording						●	
Inform	Dynamic Privacy Policy Display						●	
Inform	Privacy icons	●	●					●
Inform	Icons for Privacy Policies		●				●	
Inform	Layered Policy Design		●				●	
Inform	Privacy Labels						●	
Inform	Privacy Policy Display							●
Inform	Impactful Information and Feedback	●					●	●
Inform	Platform for Privacy Preferences			●				●
Inform	Policy Matching Display			●				●
Inform	Privacy-Aware Network Client						●	
Inform	Increasing awareness of information aggregation							●
Inform	Informed Credential Selection							●
Inform	Informed Secure Passwords	●	●			●	●	●
Inform	Unusual Activities			●				●
Inform	Informed Implicit Consent		●				●	●
Inform	Minimal Information Asymmetry		●					●
Inform	Personal Data Table						●	
Inform	Preventing mistakes or reducing their impact						●	●
Inform	Privacy Awareness Panel						●	●
Inform	Privacy dashboard						●	●
Inform	Privacy Color Coding						●	
Inform	Privacy Mirrors						●	●
Inform	Trust Evaluation of Services Sides						●	
Inform	Who’s Listening						●	●
Enforce	Federated Privacy Impact Assessment	●	●	●			●	
Enforce	Obligation Management	●		●			●	
Enforce	Sticky Policies			●				●
Enforce	Identity Federation Do Not Track Pattern	●	●	●				

Quadro 54. Mapeamento dos Padrões de Privacidade e Princípios do PbD – Participante C

Participante C								
Estratégia de Hoepman	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Abstract	Location Granularity	●	●	●				●
Control	Decoupling [content] and location information visibility	●		●			●	●
Control	Active broadcast of presence	●		●			●	●
Control	Buddy List				●			●
Control	Discouraging blanket strategies	●	●	●				●
Control	Enable/Disable Functions			●				●
Hide Control	Encryption with user-managed keys	●	●	●		●		
Control	Incentivized Participation		●					●
Inform Control	Informed Consent for Web-based Transactions				●		●	●
Control	Lawful Consent	●		●			●	●
Control	Masquerade	●	●	●		●		●
Control	Negotiation of Privacy Policy	●					●	●
Control	Outsourcing [with consent]	●					●	
Control	Pay Back			●				●
Control	Obtaining Explicit Consent						●	●
Separate Control	Personal Data Store			●			●	●
Control	Private link	●	●	●				
Control	Reasonable Level of Control	●		●			●	●
Control	Reciprocity			●			●	●
Control	Selective access control		●	●			●	●
Control	Selective Disclosure	●	●	●				●
Control	Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context						●	●
Control	Single Point of Contact	●	●			●	●	●
Separate	User data confinement pattern	●					●	●
Minimize Hide	Added-noise measurement obfuscation	●	●	●				
Hide	Aggregation Gateway	●	●	●		●		
Hide	Trustworthy Privacy Plug-in	●	●	●		●		
Hide	Anonymity Set	●	●					
Hide Separate	Anonymous Reputation-based Blacklisting		●	●	●			
Hide	Onion Routing	●	●			●		
Hide	Pseudonymous Identity	●	●	●	●			
Hide	Pseudonymous Messaging	●	●	●		●		
Hide	Use of dummies		●	●				
Hide	Attribute Based Credentials	●	●					●
Minimize	Protection against Tracking	●	●					●

Minimize	Strip Invisible Metadata	●		●	●		●	
Inform	Abridged Terms and Conditions	●						●
Inform	Appropriate Privacy Icons						●	
Inform	Ambient Notice						●	●
Inform	Appropriate Privacy Feedback	●	●				●	●
Inform	Asynchronous notice						●	●
Inform	Awareness Feed	●	●				●	●
Inform	Data Breach Notification Pattern	●					●	●
Inform	Privacy Aware Wording			●				●
Inform	Dynamic Privacy Policy Display						●	
Inform	Privacy icons			●			●	●
Inform	Icons for Privacy Policies						●	
Inform	Layered Policy Design						●	
Inform	Privacy Labels	●					●	●
Inform	Privacy Policy Display						●	
Inform	Impactful Information and Feedback	●					●	●
Inform	Platform for Privacy Preferences			●			●	●
Inform	Policy Matching Display		●				●	●
Inform	Privacy-Aware Network Client						●	
Inform	Increasing awareness of information aggregation						●	●
Inform	Informed Credential Selection						●	●
Inform	Informed Secure Passwords	●				●	●	●
Inform	Unusual Activities	●					●	●
Inform	Informed Implicit Consent	●	●				●	●
Inform	Minimal Information Asymmetry	●	●				●	●
Inform	Personal Data Table						●	●
Inform	Preventing mistakes or reducing their impact						●	●
Inform	Privacy Awareness Panel	●					●	●
Inform	Privacy dashboard	●					●	●
Inform	Privacy Color Coding						●	
Inform	Privacy Mirrors						●	●
Inform	Trust Evaluation of Services Sides						●	
Inform	Who’s Listening	●	●				●	●
Enforce	Federated Privacy Impact Assessment	●		●				
Enforce	Obligation Management	●		●			●	
Enforce	Sticky Policies	●		●			●	
Enforce	Identity Federation Do Not Track Pattern	●		●				

APÊNDICE F – MAPEAMENTO ENTRE PADRÕES DE PRIVACIDADE E PRINCÍPIOS DO PRIVACY BY DESIGN

O Quadro 55 apresenta os Padrões de Privacidade associados às estratégias *Separate*, *Hide*, *Minimize* e *Enforce*. As linhas que apresentam o caractere (●) indicam que o padrão de privacidade em questão contempla o princípio do PbD respectivo à coluna. Por outro lado, sua ausência indica a não relação.

Quadro 55. Resultado do Mapeamento entre Padrões de Privacidade e Princípios do PbD relacionados às estratégias *Separate*, *Hide*, *Minimize* e *Enforce*

Estratégia de Hoepman (2014)	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Separate	User data confinement pattern	●	●	●				
Minimize Hide	Added-noise measurement obfuscation	●	●	●				
Hide	Aggregation Gateway	●	●	●		●		
Hide	Trustworthy Privacy Plug-in	●	●	●		●		
Hide	Anonymity Set	●	●					
Hide Separate	Anonymous Reputation-based Blacklisting	●	●	●	●			
Hide	Onion Routing	●	●	●		●		
Hide	Pseudonymous Identity	●	●	●	●			
Hide	Pseudonymous Messaging	●	●	●		●		
Hide	Use of dummies		●	●				
Hide	Attribute Based Credentials	●	●					●
Minimize	Protection against Tracking	●		●				●
Minimize	Strip Invisible Metadata	●	●	●	●			
Enforce	Federated Privacy Impact Assessment	●		●				
Enforce	Obligation Management	●		●			●	
Enforce	Sticky Policies	●		●			●	
Enforce	Identity Federation Do Not Track Pattern	●		●				

Quando a coleta de dados pessoais representa uma ameaça a privacidade dos titulares, pode-se repensar a arquitetura do sistema. O padrão User Data Confinement Pattern estabelece uma alteração na relação de confiança entre titulares de dados e provedores de serviços. Em vez dos dados pessoais dos titulares serem coletados e processados pelo provedor de serviço, o processamento ocorre localmente no ambiente confiável do usuário, isso permite um maior controle dos dados pessoais por parte dos titulares. Neste contexto, o padrão User Data Confinement Pattern

contempla os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão e Privacidade Incorporada ao Design.

O padrão Added-Noise Measurement Obfuscation visa adicionar um valor de ruído ao valor verdadeiro de um atributo coletado do titular do dado antes de transmiti-lo. Assim, ao obter o dado, um terceiro não seria capaz de inferir o valor correto ao mesmo, preservando a privacidade do titular. Desse modo, o padrão Added-Noise Measurement Obfuscation está relacionado aos princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, e Privacidade Incorporada ao Design.

A adequação de um determinado serviço aos seus usuários pode exigir medições detalhadas de atributos dos titulares de dados. Quando essas medições são realizadas ao longo do tempo, podem revelar hábitos pessoais dos usuários. Com isso, o padrão Aggregation Gateway menciona que os dados dos titulares podem ser agrupados e criptografados utilizando criptografia homomórfica. Assim, o provedor de serviço terá acesso confiável aos dados de modo que atenda seus requisitos operacionais, porém, sem permitir que acesse individualmente os dados de cada usuário. Com isso, o padrão Aggregation Gateway abrange os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Segurança de Ponta a Ponta.

Neste mesmo contexto, em que hábitos pessoais dos titulares de dados podem coletados por meio de medições repetidas e detalhadas de um determinado atributo, o padrão Trustworthy Privacy Plug-in menciona a instalação de um *plugin* no dispositivo do titular a fim de realizar a coleta e processamento das informações localmente e de controle do próprio titular dos dados, enviando, de modo criptografado, ao servidor do prestador de serviços apenas os dados agregados em alta granularidade. Desse modo, o padrão Trustworthy Privacy Plug-in compreende os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Segurança de Ponta a Ponta.

O padrão Anonymity Set tem como objetivo não permitir que um titular dos dados seja distinguido entre os demais usuários de um serviço. Para isso, o padrão estabelece a remoção de quaisquer características específicas dos titulares ou, se o número dos usuários for limitado, deve-se inserir identidades falsas a fim de tornar inviável a distinção entre eles. Portanto, o padrão Anonymity Set inclui os princípios Proativo não Reativo; Prevenir não Remediar e Privacidade por Padrão.

A fim de possibilitar que o titular dos dados utilize um determinado serviço de maneira anônima, porém, sem promover o mal comportamento do mesmo, uma vez que não pode ser identificável, o padrão Anonymous Reputation-Based Blacklisting determina que o provedor do serviço forneça credenciais anônimas aos usuários e atribua uma pontuação de reputação com base na sessão estabelecida. Caso a reputação desta sessão seja negativa, a mesma é adicionada à uma lista com as sessões infratoras, impossibilitando que o usuário continue a utilizar o serviço. Dessa maneira, o padrão Anonymous Reputation-Based Blacklisting engloba os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Funcionalidade Total.

Quando determinados dados são enviados em uma rede, os nós intermediários devem ter conhecimento do nó remetente e receptor, infringindo princípios de privacidade de dados. Dessa maneira, o padrão Onion Routing determina o uso de criptografia dos dados em camadas de modo que cada nó possa remover apenas uma camada para ter conhecimento do próximo nó na rede. Sendo assim, o padrão Onion Routing abarca os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Segurança de Ponta a Ponta.

O padrão Pseudonymous Identity tem como intuito ocultar a identidade verdadeira de um titular dos dados por meio da atribuição de pseudônimos. Assim, é possível que usuários de um determinado serviço possam enviar informações confidenciais, como por exemplo, dados de localização, mensagens em fóruns, entre outros, sem que seja possível relacionar o pseudônimo a identidade real do titular. Neste contexto, o padrão Pseudonymous Identity compreende os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Funcionalidade Total.

Por sua vez, o padrão Pseudonymous Messaging soluciona o problema de que mensagens enviadas por meio de canais de comunicações podem ser armazenadas e utilizadas contra o seu autor. Como solução, o padrão menciona a criação de um servidor que recebe a mensagem do remetente e substitui o endereço dele por um pseudônimo. Quando esta mensagem for respondida, ela será enviada ao endereço mascarado, que será trocado novamente para o endereço original. Desse modo, o padrão Pseudonymous Messaging contempla os princípios Proativo não Reativo;

Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Segurança de Ponta a Ponta.

O padrão Use of Dummies tem como intuito ofuscar as ações do titular dos dados em um determinado serviço. Para isso, o padrão realiza execuções simultâneas de ações aleatórias a fim de impossibilitar que terceiros distingam quais ações são reais ou falsas. Com isso, o padrão Use of Dummies está relacionado com os princípios Privacidade por Padrão e Privacidade Incorporada ao Design.

Normalmente, o provedor de serviços necessita realizar autenticações de seus usuários a fim de permitir que ele faça uso de funcionalidades da aplicação. Porém, ao solicitar informações pessoais ao titular de dados a fim de autenticá-lo, atributos desnecessários podem ser apresentados, não preservando a privacidade do usuário. Neste contexto, o padrão Attribute Based Credentials estabelece a criação dos chamados “Emissores de Credenciais”, os quais são utilizados pelos titulares de dados para emitir credenciais de autenticação. Os emissores de credenciais geram *tokens* que comprovam, aos provedores de serviços, que a informações pessoais do usuário estão corretas e atendem às políticas de controle de autenticação para o serviço em questão, sem expor informações adicionais do titular de dados. Portanto, o padrão Attribute Based Credentials inclui os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão e Respeito pela Privacidade do Usuário.

O padrão Protection Against Tracking procura restringir o uso de *cookies* no lado do cliente a fim de proteger os titulares de dados contra rastreamento de seu comportamento em *websites*. Porém, respeita os interesses do usuário pois permite que o titular de dados habilite os *cookies* da maneira que melhor o convém. Sendo assim, o padrão Protection Against Tracking contempla os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Quando o serviço possibilita que os titulares realizem *uploads* de arquivos pessoais, como por exemplo, documentos, fotos, entre outros, diferentes metadados podem estar relacionados aos arquivos importados, desta maneira, a privacidade dos dados pessoais dos titulares são colocadas em risco. Neste contexto, o padrão Strip Invisible Metadata possibilita remover os metadados dos arquivos pessoais o que auxilia na proteção da privacidade dos titulares sem comprometer a funcionalidade do sistema, além de antecipar futuros problemas contra vazamento de informações, pois

aqueles arquivos não carregam consigo os dados pessoais dos titulares. Sendo assim, o padrão Strip Invisible Metadata abrange os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Privacidade Incorporada ao Design e Funcionalidade Total.

Nos cenários em que o provedor de identidade e de serviços são separados, a identidade dos titulares de dados é armazenada em diferentes sistemas, os quais configuram uma “federação”. Entretanto, a complexidade do fluxo de dados entre os elementos da federação implica em novos riscos e ameaças aos dados pessoais. Com isso, o padrão Federated Privacy Impact Assessment tem como intuito realizar uma avaliação de impacto a privacidade por todos os membros da federação, individualmente e eu conjunto a fim de definir políticas de privacidade compartilhadas e comprovar o seu cumprimento. Portanto, o padrão Federated Privacy Impact Assessment abarca os princípios Proativo não Reativo; Prevenir não Remediar e Privacidade Incorporada ao Design.

Os dados pessoais dos titulares são acessados ou tratados por várias partes que os compartilham. Para isso, ambos os padrões Obligation Management e Sticky Policies definem aos prestadores de serviços utilizar um sistema de gerenciamento de obrigações que considera as preferências individuais dos titulares na manipulação dos seus dados pessoais durante todo o ciclo de vida dos dados, garantindo a minimização, eliminação e notificação aos titulares quando seus dados forem manipulados. Dessa maneira, os padrões Obligation Management e Sticky Policies compreendem os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design e Visibilidade e Transparência.

Os provedores de serviços devem diferenciar os usuários que fazem uso de seus serviços, para isso, informações pessoais são requeridas aos titulares de dados, podendo comprometer a sua privacidade, pois, mesmo que apenas algumas informações pessoais sejam compartilhadas com terceiros, correlações podem ser feitas e informações adicionais do usuário podem ser obtidas. Sendo assim, o padrão Identity Federation Do Not Track Pattern estabelece a criação do “orquestrador”, que atua e é controlado pelo titular de dados. O orquestrador tem a função de garantir que a correlação de identidade só possa ocorrer por meio dele, assegurando a privacidade do titular. Neste contexto, o padrão Identity Federation Do Not Track Pattern contempla os princípios Proativo não Reativo; Prevenir não Remediar e Privacidade Incorporada ao Design.

Por fim, o Quadro 56 aborda os Padrões de Privacidade relacionados à estratégia *Inform*.

Quadro 56. Resultado do Mapeamento entre Padrões de Privacidade e Princípios relacionados à estratégia *Inform*

Estratégia de Hoepman (2014)	Padrões de Privacidade	Princípios do *Privacy by Design*						
		1. Proativo não Reativo	2. Privacidade por Padrão	3. Privacidade Incorporada no Design	4. Funcionalidade Total	5. Segurança Ponta a Ponta	6. Visibilidade e Transparência	7. Respeito pela Privacidade do Usuário
Inform	Abridged Terms and Conditions						●	
Inform	Appropriate Privacy Icons						●	
Inform	Ambient Notice	●		●			●	●
Inform	Appropriate Privacy Feedback						●	●
Inform	Asynchronous notice						●	●
Inform	Awareness Feed						●	●
Inform	Data Breach Notification Pattern						●	●
Inform	Privacy Aware Wording						●	
Inform	Dynamic Privacy Policy Display						●	
Inform	Privacy icons						●	
Inform	Icons for Privacy Policies						●	
Inform	Layered Policy Design						●	
Inform	Privacy Labels						●	
Inform	Privacy Policy Display						●	
Inform	Impactful Information and Feedback						●	●
Inform	Platform for Privacy Preferences			●				●
Inform	Policy Matching Display			●				●
Inform	Privacy-Aware Network Client						●	
Inform	Increasing awareness of information aggregation						●	●
Inform	Informed Credential Selection						●	●
Inform	Informed Secure Passwords	●				●		●
Inform	Unusual Activities			●				●
Inform	Informed Implicit Consent						●	●
Inform	Minimal Information Asymmetry	●	●				●	●
Inform	Personal Data Table						●	●
Inform	Preventing mistakes or reducing their impact						●	●
Inform	Privacy Awareness Panel						●	●
Inform	Privacy dashboard						●	●
Inform	Privacy Color Coding						●	
Inform	Privacy Mirrors						●	●
Inform	Trust Evaluation of Services Sides						●	
Inform	Who's Listening						●	●

Termos e condições de usos de serviços são escritos de maneira que dificultam o entendimento dos usuários e, por isso, são ignorados. Porém, os controladores

necessitam que os titulares dos dados tomem ciência dos riscos, direitos e responsabilidades da utilização do sistema, principalmente em relação a privacidade de dados, e concedam seu consentimento com a utilização de seus dados pessoais. O padrão Abridged Terms and Conditions busca resumir os termos e condições de um determinado serviço ao usuário de modo que ele tenha interesse em lê-los e compreender os riscos de sua utilização. Portanto, o padrão Abridged Terms and Conditions inclui apenas o princípio Visibilidade e Transparência.

Um modo de resumir os termos e condições, como abordado pelo padrão Abridged Terms and Conditions, é o uso de ícones de privacidade. Porém, estes podem ser mal interpretados pelos usuários do sistema devido sua natureza subjetiva ou, mesmo que totalmente compreendidos, detalhes importantes podem ser negligenciados. Para solucionar este problema, o padrão Appropriate Privacy Icons menciona que deve ser apresentado um conjunto consistente de ícones, cuidadosamente agrupados e não excessivos, além de explicações curtas e concisas dos seus significados. Com isso, o padrão Appropriate Privacy Icons está relacionado apenas ao princípio Visibilidade e Transparência.

O padrão Ambient Notice tem como objetivo notificar o titular de dados que seus dados pessoais estão sendo coletados, seja por meio de um sensor, câmera ou outro periférico. Além disso, ao elicitar um determinado requisito de software que necessita de uma leitura ou uso de periférico que coletará dados pessoais do titular, deve-se obter o consentimento do mesmo, notificá-lo sobre a coleta de informações e permitir que o próprio titular revogue o consentimento a qualquer instante. Sendo assim, o padrão Ambiente Notice contempla os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade Incorporada ao Design, Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Alguns serviços são projetados para continuar sua execução em segundo plano, porém, isso faz com que informações sejam coletadas e processadas sem que os titulares dos dados tenham conhecimento, mesmo que desejem obter os benefícios do serviço. O padrão Appropriate Privacy Feedback estabelece ciclos de *feedbaks* visíveis que chamem a atenção do titular de dados para garantir que ele entenda quais dados estão sendo coletados, quem pode acessar e como estão sendo utilizados. Neste contexto, o padrão Appropriate Privacy Feedback está relacionado aos princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

O padrão Asynchronous Notice tem como intuito notificar o titular que seus dados pessoais estão sendo coletados mesmo que ele tenha consentido anteriormente. Isso se dá pelo fato de que usuários estarem sujeitos ao esquecimento ou porque o consentimento foi dado por outra pessoa que compartilha o mesmo dispositivo. Essa notificação deve ocorrer por avisos assíncronos aleatórios enviados, por exemplo, uma vez por semana em horários diferentes, dificultando que um invasor esconda o aviso. Neste contexto, o padrão Asynchronous Notice abrange os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

As organizações possuem produtos e/ou serviços que estão constantemente em evolução para fornecer uma maior comodidade e qualidade aos seus usuários. Porém, ao inserir uma nova funcionalidade em nos sistemas, a privacidade de dados pessoais dos titulares pode ser coloca em risco, mesmo que estes tenham consentido com determinadas coletas de seus dados pessoais. Desse modo, o padrão Awareness Feed menciona que avisos aos titulares dos dados sobre possíveis consequências devem ser emitidos antes de realizar a coleta e processamento dos dados pessoais. Além disso, não deve permitir que o usuário faça uso das novas funcionalidades sem que aceite os termos de utilização. Com isso, o padrão Awareness Feed inclui os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Por outro lado, quando ocorrem violações de dados, o padrão Data Breach Notification Pattern estabelece que os controladores dos dados devem detectar e reagir rapidamente, notificando às autoridades supervisoras a natureza e extensão dos dados afetados, prováveis consequências e medidas propostas para mitigar os efeitos da violação. Caso os titulares dos dados também sejam afetados, eles devem ser informados. Por fim, a violação deve ser documentada para revisão futura. Portanto, o padrão Data Breach Notification Pattern engloba os princípios termos de utilização. Com isso, o padrão Awareness Feed inclui os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Ao utilizar o determinado serviço, os titulares de dados recebem informações sobre as políticas de privacidade a fim de informá-los sobre a finalidade para que os seus dados pessoais serão coletados, processados e armazenados. No entanto, há muitos detalhes, além da complexidade do conteúdo e vocabulário, o que compromete a validade do consentimento do titular. Com isso, o padrão Privacy Aware Wording recomenda o uso de termos padronizados além da realização de testes de usuário

sobre a compreensão dos termos e frases utilizados a fim de simplificar os textos das políticas de privacidade. Neste contexto, o padrão Privacy Aware Wording abrange apenas o princípio Visibilidade e Transparência.

O problema de políticas de privacidade abordarem textos completos em seu conteúdo e vocabulário também é abordado pelo padrão Dynamic Privacy Policy Display, porém, este padrão tem como intuito fornecer ao titular dos dados apenas informações relevantes da política de privacidade e, ao passar o mouse ou pressionar para saber mais, é apresentado mais detalhes daquele tópico. As informações devem ser exibidas de maneira consistente e destacar as possíveis consequências da divulgação de informações pessoais. Dessa maneira, o padrão Dynamic Privacy Policy Display abarca apenas o princípio Visibilidade e Transparência.

Além do padrão Dynamic Privacy Policy Display, os padrões Privacy Icons e Icons for Privacy Policies também permitem fornecer de uma maneira simplificada as políticas de privacidade ao usuário. Enquanto o padrão Privacy Icons oferece como solução a inserção de ícones como complemento do texto, o padrão Icons for Privacy Policies estabelece o agrupamento, descrição e organização das políticas de privacidade por meio de ícones. Em ambos os casos os ícones devem ser consistentes e padronizados, não permitindo interpretações errôneas. Além disso, os ícones, de maneira alguma, devem ser utilizados em substituição ao documento de política de privacidade. Sendo assim, tanto o padrão Privacy Icons quanto o padrão Icons for Privacy Policies compreendem apenas o princípio Visibilidade e Transparência.

Semelhante aos padrões Dynamic Privacy Policy Display e Icons for Privacy Policies, o padrão Layered Policy Design tem como objetivo extrair em um primeiro plano aspectos cruciais da política de privacidade de um determinado serviço. Um breve resumo das práticas que tratam a privacidade de dados pessoais deve estar em um primeiro plano, dividido em seções. Assim, se o usuário necessitar de informações específicas de uma destas seções, ele poderá consultar maiores detalhes daquele assunto e até mesmo o texto legal na íntegra da política de privacidade. Portanto, o padrão Layered Policy Design inclui apenas o princípio Visibilidade e Transparência.

Uma solução semelhante para auxiliar a compreensão das políticas de privacidade pelos titulares, é a utilização de rótulos coloridos. Desta maneira, os usuários podem identificar pela cor se aquela informação diz respeito à coleta, armazenamento, processamento, compartilhamento, entre outros, conforme

estabelece o padrão Privacy Labels. Com isso, o padrão Privacy Labels está relacionado apenas ao princípio Visibilidade e Transparência.

Outra possibilidade de apresentar as políticas de privacidade aos usuários, é apresentada pelo padrão Privacy Policy Display, que estabelece que à medida que os dados pessoais são solicitados, deve-se indicar claramente quais informações são necessárias e quais serão as finalidades, antes de solicitar o consentimento do titular de dados. Portanto, o padrão Privacy Policy Display abrange apenas o princípio Visibilidade e Transparência.

Por sua vez, o padrão Impactful Information and Feedback visa analisar o conteúdo do titular de dados a fim de fornecer informações e sugestões relevantes ao mesmo antes dele divulgar suas informações. Esta análise pode ocorrer via processamento de linguagem natural e, mesmo que o usuário ignore as informações apresentadas, deve permitir a ele que indique que se arrependeu da postagem, caso seja de sua vontade. Neste contexto, o padrão Impactful Information and Feedback contempla os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

A fim de facilitar a leitura e entendimento com as políticas de privacidade, as quais são extensas, complexas e de difícil compreensão por parte dos usuários, o padrão Platform for Privacy Preferences sugere que os controladores utilizem a padronização P3P para construí-las. Pois, uma vez que estas políticas são definidas e compartilhadas com outros controladores, os usuários poderão definir preferências de privacidade e, quando se deparar com uma nova política, poderão revisar de maneira direta apenas detalhes que ainda não consentiram anteriormente. Portanto, o padrão Platform for Privacy Preferences inclui os princípios Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

De modo semelhante ao padrão Platform for Privacy Preferences, o padrão Policy Matching Display visa auxiliar os titulares de dados em suas preferências da política de privacidade, uma vez que em diferentes serviços fornecidos pelos controladores as políticas de privacidade são semelhantes entre si. Com isso, o padrão Policy Matching Display estabelece que os controladores devem recuperar as preferências da polícia do usuário e usá-las para destacar as contradições com a política de privacidade e, se possível, definir as configurações do aplicativo com os valores que melhor atendem essas preferências. Dessa maneira, o padrão Policy

Matching Display engloba os princípios Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

A fim de simplificar a leitura e compreensão das políticas de privacidade de diferentes serviços utilizados pelos usuários, o padrão Privacy-Aware Network Client tem como objetivo implementar um *proxy* de preservação de privacidade que analisa e interpreta com segurança as políticas de privacidade, fornecendo aos usuários resumos padronizados e de fácil compreensão. Para a comunicação entre usuários e seus *proxies*, deve ser implementado um canal de comunicação seguro a fim de evitar a interceptação por terceiros. Sendo assim, o padrão Privacy-Aware Network Client abarca apenas o padrão Visibilidade e Transparência.

O padrão Increasing Awareness of Information Aggregation concede ao titular de dados informações sobre agregação de dados e como esta técnica auxilia evitar o compartilhamento excessivo de informações indesejáveis. Esta apresentação pode ser realizada por meio de exemplos hipotéticos e, posteriormente, o titular pode consentir em ter seus dados agregados pelos controladores de um determinado serviço. Desse modo, o padrão Increasing Awareness of Information Aggregation está relacionado aos princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Os controladores, por vezes, precisam impedir que usuários não autenticados tenham acessos a determinadas funcionalidades do sistema. Por outro lado, os usuários não desejam fornecer mais informações do que o necessário. Desse modo, o padrão Informed Credential Selection permite que um usuário se identifique de maneira granular, controlando a quantidade de informações pessoais que serão utilizadas, além de quem poderá acessá-las. Com isso, o padrão Informed Credential Selection abrange os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Ainda se tratando de autenticações, o padrão Informed Secure Passwords menciona que, ainda que existem outras maneiras, as senhas ainda são consideradas convenientes aos usuários. Porém, para manter os titulares de dados seguros, as senhas devem ser consideradas fortes, além de serem atualizadas frequentemente. Para isso, o padrão estabelece de modo proativo algumas recomendações para a segurança dos dados pessoais dos titulares, como por exemplo, o fornecimento de assistências na compreensão e manutenção das senhas aos usuários por meio de mecanismos passivos, estativos e dinâmicos. Dessa maneira, o padrão Informed

Secure Passwords engloba os princípios Proativo não Reativo; Prevenir não Remediar, Segurança de Ponta a Ponta e Respeito pela Privacidade do Usuário.

A autenticação por nome de usuário e senha é considerada, por muitos usuários, como fácil e rápida. Entretanto, este tipo de autenticação não fornece um nível satisfatório de segurança, pois as senhas tornam-se inseguras quando permanecem inalteradas. Neste contexto, o padrão Unusual Activities visa o equilíbrio entre a insegurança da autenticação de nome de usuário e senha e a inconveniência da autenticação multifator. Como solução é apresentada a utilização de informações disponíveis e consentidas pelo titular de dados para estabelecer uma norma de acesso, como localização, preferências, idiomas, endereço IP, entre outros. Portanto, o padrão Unusual Activities contempla os princípios Privacidade Incorporada ao Design e Respeito pela Privacidade do Usuário.

Em alguns casos, os controladores precisam coletar e processar informações dos titulares para cumprir seus interesses legítimos, como por exemplo, na detecção de fraudes ou filmagens de segurança nas instalações do próprio controlador. Nestes casos, o padrão Informed Implicit Consent fornece ao titular de dados um aviso claro e conciso de que, ao utilizar o serviço, ele consente implicitamente com o processamento necessário para atender a interesses legítimos. Este aviso deve ser notado pelo usuário antes da aplicação dos efeitos que ele descreve. Portanto, o padrão Informed Implicit Consent inclui os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Os usuários, ao utilizar um determinado serviço pela primeira vez, sabem pouco de sua da política de privacidade. Por outro lado, os controladores coletam dados do usuário, o que gera um desequilíbrio de informações. Dessa maneira, o padrão Minimal Information Asymmetry estabelece que o controlador solicite apenas informações mínimas necessárias para que o usuário consiga utilizar o serviço. Esta solicitação deve ser explicada e consentida para que seja armazenada e processada. Além disso, as políticas de privacidade devem ser descritas de maneira clara e concisa em vez de complexas com jargões jurídicos. Sendo assim, o padrão Minimal Information Asymmetry engloba os princípios Proativo não Reativo; Prevenir não Remediar, Privacidade por Padrão, Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

O padrão Personal Data Table tem como intuito apresentar aos titulares de como seus dados pessoais estão sendo armazenados, processados e

compartilhados. Para isto, o padrão estabelece o uso de tabelas contendo informações como: quais dados foram coletados, por quê foram coletados, qual finalidade, quem possui acesso, quais consentimentos foram dados, entre outras informações. Estas informações podem ser filtradas e organizadas de acordo com a necessidade de cada titular. Além disso, esta tabela poderá conter links para outras páginas/telas que permitam aos usuários alterar duas configurações de privacidade. Neste contexto, o padrão Personal Data Table abarca os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Em determinados serviços, os usuários desejam compartilhar suas informações pessoais ou conteúdos em geral com terceiros. A fim de simplificar as configurações de compartilhamento dos usuários a cada publicação, eles podem definir uma configuração que serão aplicadas as publicações seguintes. Porém, a não confirmação de consentimento do titular sobre as configurações de compartilhamento pode leva-lo à divulgação de dados pessoais de maneira não intencional. Desse modo, o padrão Preventing Mistakes or Reducing Their Impact estabelece estudos de padrões no comportamento de divulgação, pois se ocorrer uma mudança potencialmente significativa no contexto das publicações de um usuário, o mesmo poderá ser alertado a revisar as configurações de compartilhamento. Com isso, o padrão Preventing Mistakes or Reducing Their Impact compreende os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Principalmente em serviços web, usuários podem ter a falsa impressão de que suas atividades são anônimas, porém, os controladores e demais usuários podem ter acesso à detalhes, como histórico de publicação, versão do navegador, endereço IP, entre outros. Para que estes usuários não sejam surpreendidos, o padrão Privacy Awareness Panel recomenda o uso de painéis para mostrar aos usuários as informações relacionadas ao navegador, como sessões, IP e metadados que possam identifica-los. Além disso, lembretes aos usuários de quem poderá visualizar o conteúdo que está sendo divulgado, qual será o processamento do mesmo e quais informações os controladores obtêm dele também podem constar no painel. Portanto, o padrão Privacy Awareness Panel comtempla os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

Semelhante ao padrão Privacy Awareness Panel, o padrão Privacy Dashboard concede ao titular de dados um painel de privacidade no qual são apresentados registros, relatórios, notificações sobre os dados pessoais coletados e armazenados

e informações relevantes sobre a agregação dos dados. Além disso, o painel deve possibilitar ao usuário atualizar seus dados pessoais ou excluí-los, se achar conveniente. Sendo assim, o padrão Privacy Dashboard abrange os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

A fim de simplificar as configurações de preferências de privacidade de dados, o padrão Privacy Color Coding visa o uso de cores padronizadas para orientar o titular de dados na seleção de configurações amigáveis à privacidade. Cada cor é atribuída a diferentes níveis de privacidade, como por exemplo, uma publicação pública pode assumir a cor vermelha, como um sinal de alerta. Dessa maneira, o padrão Privacy Color Coding está relacionado apenas ao princípio Visibilidade e Transparência.

O padrão Privacy Mirrors fornece um *framework* sociotécnico que permite aos usuários receber registros, relatórios e outros acessos informativos relevantes sobre o uso de seus dados pessoais. Para isto, os usuários podem configurar o meio que desejam receber as informações, como por exemplo, e-mail, notificação ou pela própria interface do sistema. Sendo assim, o padrão Privacy Mirrors abrange os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

A confiança dos usuários em um determinado serviço é primordial para o sucesso da companhia, visto que sem ela, os usuários buscam alternativas ou geram publicidade negativa. Para isto, o padrão Trust Evaluation of Services Sides visa fornecer informações sobre a confiabilidade do serviço e de terceiros que estão a ele vinculados. As qualidades apresentadas podem ser coletadas por meio de avaliações independentes em diversos critérios. Dessa maneira, permite aos titulares de dados receber informações extras no momento da obtenção de consentimento informado, garantindo que não tomem decisões equivocadas. Neste contexto, o padrão Trust Evaluation of Services Sides inclui apenas o princípio Visibilidade e Transparência.

Os usuários de serviços frequentemente compartilham seu uso com terceiros, pessoas conhecidas, desconhecidas, anônimas ou não autenticadas, principalmente em ambientes colaborativos. Para estes casos, em que o titular de dados não sabe se o conteúdo que acessam ou divulgam foi acessado ou modificado por terceiros, o padrão Who's Listening estabelece informar ao titular que outros usuários, mesmo aqueles que não se encontram autenticados, estão acessando o conteúdo em questão. Esta informação pode ser apresentada por meio do nome de usuário, foto de perfil, avatar, iniciais do nome ou "anônimo". Além disso, cada usuário pode modificar se será identificado ou permanecerá anônimo, preservando assim, sua privacidade.

Desse modo, o padrão Who's Listening engloba os princípios Visibilidade e Transparência e Respeito pela Privacidade do Usuário.

APÊNDICE G – REPOSITÓRIO DE INSTÂNCIAS DE PADRÕES DE PRIVACIDADE

Enable/Disable Functions

Mariana utiliza um navegador de internet para acessar diversos *websites* no seu dia a dia. Porém, o navegador registra todo o histórico de navegação, histórico de download, buscas, senhas, dados de formulários, entre outros dados pessoais de Mariana, que diariamente realiza uma limpeza dos dados coletados pelo sistema.

Mariana deseja que o navegador possibilite escolher quais funcionalidades gostaria de manter habilitadas no sistema e quais deixaria desabilitadas para minimizar a coleta de seus dados pessoais. Para isto, o padrão de privacidade Enable/Disable Functions pode ser aplicado, informando à Mariana quais são as funcionalidades opcionais no sistema e quais dados pessoais cada funcionalidade coleta e, ao habilitar uma determinada funcionalidade, o usuário estará consentindo com a coleta dos dados mencionados. A Figura 38 detalha a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ser capaz de ativar e desativar a função de registro de histórico de navegação.
Para que eu possa controlar quais informações são coletadas sobre minha navegação na web.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Histórico de navegação.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- A funcionalidade de ativar/desativar o registro de histórico deve ser claramente identificável e facilmente acessível a partir da interface do usuário.
- Quando a função de registro de histórico é desativada, o navegador não deve mais coletar informações sobre as páginas visitadas e outras atividades de navegação.
- O status atual da função de registro de histórico deve ser claramente indicado na interface do usuário.
- Quando a função de registro de histórico é ativada, deve haver uma clara notificação sobre quais dados serão coletados e como serão utilizados, juntamente com uma opção de consentimento explícito antes que o registro comece.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Enable/Disable Functions.</td></tr>
</table>

Figura 38. História de Usuário Utilizando o Padrão de Privacidade Enable/Disable Functions.

Encryption With User-Managed Keys

Mário gostaria de realizar backup de seus arquivos pessoais utilizando um serviço de armazenamento na nuvem. Porém, ele tem receio que seus arquivos fiquem vulneráveis a acessos de terceiros. Um modo de contornar esta situação é criptografar seus dados armazenados. Entretanto, Mário quer ter controle total sobre as chaves de criptografias, ou seja, as chaves deverão ser armazenadas e gerenciadas por ele.

Neste contexto, pode-se utilizar o padrão de privacidade Encryption With User-Managed Keys que possibilita ao próprio titular de dados gerar e gerenciar uma chave de criptografia antes de armazenar e transferir os arquivos pessoais. A Figura 39 apresenta a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero realizar backup de arquivos em serviços na nuvem.
Para que eu possa garantir a segurança e disponibilidade dos meus arquivos.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Senha.
- Chave de Criptografia.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- As informações pessoais do usuário devem ser criptografadas antes de serem armazenadas ou transferidas.
- A chave de criptografia deve ser fornecida ao usuário, que deve ser responsável por gerenciá-la.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Encryption with User-Managed Keys.</td></tr>
</table>

Figura 39. História de Usuário Utilizando o Padrão de Privacidade Encryption With User-Managed Keys.

Incentivized Participation

O governo federal lançou um aplicativo que visa facilitar o acesso do cidadão aos serviços públicos digitais. É por meio deste aplicativo que o governo coleta dados de seus cidadãos para realizar censos demográficos, verificar condições de vida da população, entre outros.

Porém, alguns meses se passaram e a adesão ao aplicativo está baixa, impactando negativamente no propósito do sistema. Neste cenário, o padrão de

privacidade Incentivized Participation pode ser utilizado para promover o engajamento da população ao aplicativo do governo federal por meio do oferecimento recompensas, como por exemplo, abatimento no imposto de renda ao cidadão que utilizar ativamente o sistema e consentir com a coleta de dados pessoais. A história de usuário do exemplo supracitado é descrita na Figura 40.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero receber recompensas pelo compartilhamento de dados pessoais e engajamento no serviço utilizado.
Para que eu possa aproveitar os benefícios fornecidos pelo serviço.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- CPF.
- E-mail.
- Data de Nascimento.
- Naturalidade.
- Endereço.
- Nome da Mãe.
- Nome do Pai.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Os usuários devem consentir em compartilhar seus dados pessoais.
- Os usuários devem ser informados quais serão as recompensas recebidas.
- Deve-se definir limites na quantidade de recompensas oferecidas aos usuários.
- Os usuários devem ser informados de forma clara e transparente sobre como seus dados serão coletados, usados e compartilhados em relação à oferta de incentivos.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Incentivized Participation.</td></tr>
</table>

Figura 40. História de Usuário Utilizando o Padrão de Privacidade Incentivized Participation.

Informed Consent for Web-based Transactions

Rafael possui um aplicativo de comércio eletrônico. Ao realizar uma compra foi necessário preencher o formulário com seus dados pessoais, como nome completo, E-mail, endereço e informações de pagamento. Rafael compreendeu que aqueles dados solicitados eram necessários. Porém, dias após a realização da compra, notou que começou a receber E-mails com promoções da própria loja virtual e de lojas parceiras.

Neste contexto, o padrão de privacidade Informed Consent for Web-based Transactions pode ser utilizado, pois menciona que, ao realizar uma transação on-

line, o usuário deve ser informado quais dados pessoais serão coletados, qual a finalidade da coleta e com quem será compartilhado. Para que a transação prossiga, o usuário deverá concordar com os termos apresentados, caso contrário, a transação deverá ser interrompida e nenhum dado pode ser coletado. A Figura 41 exibe a história de usuário para o cenário descrito.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ser informado sobre quais informações são coletadas e utilizadas durante as transações on-line.
Para que eu possa consentir com o uso dos meus dados pessoais.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Data de Nascimento.
- Endereço.
- Informações de Pagamento.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Os usuários devem receber informações claras e concisas sobre quais dados pessoais serão coletados.
- Os usuários devem receber informações sobre a finalidade da coleta dos seus dados pessoais durante a transação on-line.
- Os usuários devem receber informações sobre o compartilhamento dos seus dados pessoais.
- Os usuários devem consentir com o uso dos seus dados pessoais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Informed Consent for Web-based Transactions.</td></tr>
</table>

Figura 41. História de Usuário Utilizando o Padrão de Privacidade Informed Consent for Web-based Transactions.

Lawful Consent

Rodrigo é usuário de uma rede social e está preocupado com a privacidade dos seus dados pessoais, visto que não recebe informações de quais dados estão sendo coletados e com quem estão sendo compartilhados.

Para garantir que os usuários sejam informados de maneira clara e precisa sobre o uso de suas informações pessoais e possam consentir com a política de privacidade da rede social, o padrão de privacidade Lawful Consent pode seu utilizado, pois permite ao titular de dados controlar suas informações, incluindo a capacidade de acessar, corrigir e excluir seus dados pessoais, além de revisar e retirar

o consentimento informado a qualquer momento. A Figura 42 aborda a história de usuário para o exemplo mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero que minhas informações sejam compartilhadas com terceiros apenas após obtenção de meu consentimento.
Para que meus dados pessoais não sejam utilizados indevidamente.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Fotografia.
- Data de Nascimento.
- Informações pessoais que o usuário deseja compartilhar.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Fornecer aos usuários informações de como suas informações são coletadas, armazenadas e processadas.
- Obter o consentimento explícito do usuário para realizar o tratamento de dados pessoais.
- Oferecer ao usuário mecanismos para acessar, corrigir e excluir dados pessoais, se assim ele desejar.
- Oferecer ao usuário um modo dele retirar a qualquer momento o consentimento informado.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Lawful Consent.</td></tr>
</table>

Figura 42. História de Usuário Utilizando o Padrão de Privacidade Lawful Consent.

Masquerade

Eliane deseja se comunicar com outras pessoas usando uma plataforma de mensagens instantâneas, porém não quer que sua identidade seja revelada. Ela teme que seus dados pessoais possam ser coletados ou rastreados por terceiros e que sua privacidade possa ser comprometida.

Neste cenário, o padrão de privacidade Masquerade pode ser utilizado, pois permite aos usuários escolherem mascarar sua real identidade. A Figura 43 destaca a história de usuário referente ao cenário citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero enviar mensagens de texto.
Para que eu possa me comunicar com demais usuários que fazem parte do mesmo grupo de contatos.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Telefone.</td><td>Dados Pessoais Sensíveis:
- Fotografia.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Fornecer ao usuário filtros e subconjunto de atributos que podem substituir seus dados pessoais reais.
- Possibilitar ao usuário alterar o nível de privacidade de seus dados pessoais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Masquerade.</td></tr>
</table>

Figura 43. História de Usuário Utilizando o Padrão de Privacidade Masquerade.

Negotiation of Privacy Policy

Ana gostaria de realizar compras em uma loja virtual. Porém, primeiramente precisa realizar seu cadastro na plataforma. Ao se deparar com as configurações de privacidade de seu perfil, verificou que eram muitas opções e que isso demandaria tempo, por isso deixou as configurações padrão.

Neste cenário, é preferível que as configurações padrão de privacidade protejam os dados pessoais dos usuários, visto que os usuários ainda não consentiram com o seu uso e compartilhamento. Entretanto, com a utilização de funcionalidades adicionais do sistema pode surgir a necessidade de novas informações pessoais do titular, consequentemente, o software pode solicitar o consentimento do usuário para realizar coletas e compartilhamento do que for necessário. A história de usuário do exemplo supracitado é destacada na Figura 44.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero criar uma nova conta no sistema.
Para que eu possa fazer compras pelo website.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
</table>

Restrições: - As configurações de privacidade de dados pessoais devem, por padrão, iniciar no nível mais alto de proteção. - O consentimento do usuário deve ser obtido no decorrer do uso do sistema, à medida que seja necessário coletar novos dados pessoais para oferecer demais serviços.
Recomendações de Padrões de Privacidade: - Negotiation of Privacy Policy.

Figura 44. História de Usuário Utilizando o Padrão de Privacidade Negotiation of Privacy Policy.

Outsourcing [with consent]:

O time responsável pela estratégia de uma loja on-line gostaria de melhorar seu percentual de vendas. Para este propósito, contratou-se uma empresa terceirizada de marketing a qual auxiliará no direcionamento de campanhas de publicidade para clientes em potencial com base em informações demográficas e comportamentais. Para isso, é necessário compartilhar informações pessoais dos clientes com a empresa de marketing, como nome, endereço de e-mail, idade, gênero, histórico de compras e preferências de produtos.

Como se trata de um compartilhamento de dados pessoais com terceiros, o padrão de privacidade de privacidade Outsourcing [with consent] pode ser adotado, pois será necessário informar aos clientes quais dados pessoais serão compartilhados, qual meio de compartilhamento e qual a finalidade de uso dos dados. Por fim, o compartilhamento dos dados pessoais só poderá ocorrer mediante a obtenção do consentimento do cliente. A Figura 45 descreve a história de usuário para o exemplo citado.

História de Usuário		
Como um sistema de loja on-line. **Eu quero** compartilhar os dados dos clientes com uma empresa de marketing. **Para que** ela me ajude a direcionar promoções de produtos aos meus clientes.		
Dados Pessoais: - Nome Completo. - Gênero. - E-mail. - Endereço. - Data de Nascimento. - Histórico de Compras. - Histórico de Pesquisas.	**Dados Pessoais Sensíveis:** - Gênero.	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). - Lei nº 5.172 - Sistema Tributário Nacional.		

Restrições: - Informar ao cliente quais dados pessoais, propósitos e meios do compartilhamento de dados pessoais. - O compartilhamento deverá ocorrer somente com o consentimento livre e explícito oferecido pelo titular dos dados.
Recomendações de Padrões de Privacidade: - Outsourcing [with consent].

Figura 45. História de Usuário Utilizando o Padrão de Privacidade Outsourcing [with consent].

Pay Back

Um aplicativo de saúde coleta informações pessoais dos usuários, como idade, sexo, altura, peso, dados de GPS e informações de saúde. A empresa detentora do aplicativo utiliza essas informações para recomendar produtos específicos aos seus clientes.

De acordo com o padrão de privacidade Pay Back, a empresa pode adotar uma estratégia de recompensa aos usuários do sistema que consentirem em compartilhar seus dados pessoais em troca de benefícios e descontos na compra de produtos de suplementos alimentares, em um jogo de soma positiva em que ambas as partes ganham. A Figura 46 apresenta a história de usuário para o cenário especificado.

História de Usuário		
Como um sistema de monitoramento de exercícios físicos. **Eu quero** coletar dados da saúde dos usuários. **Para que** eu possa oferecer aos usuários recomendações personalizadas de produtos fitness.		
Dados Pessoais: - Nome Completo. - E-mail. - Endereço. - Data de Nascimento. - Geolocalização.	**Dados Pessoais Sensíveis:** - Gênero. - Frequência Cardíaca. - Qualidade do Sono. - Altura. - Peso.	**Tempo de Retenção:** 20 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). - Lei nº 13.787 - Sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.		
Restrições: - Oferecer benefícios e descontos na compra de produtos suplementares comercializados pelo próprio aplicativo se o usuário consentir com a coleta de seus dados pessoais. - A coleta de dados só poderá ocorrer mediante o consentimento do titular dos dados.		
Recomendações de Padrões de Privacidade: - Pay Back.		

Figura 46. História de Usuário Utilizando o Padrão de Privacidade Pay Back.

Obtaining Explicit Consent

Henrique é um cliente de um aplicativo de entrega de alimentos. Para uma melhor experiência do usuário, o aplicativo necessita coletar alguns dados pessoais de seus usuários, como nome completo, gênero, e-mail, endereço, telefone, data de nascimento, histórico de pedido e geolocalização. Porém, os dados pessoais só podem ser coletados após o aplicativo informar ao usuário quais dados pessoais serão coletados e para que fins serão utilizados, além de obter o consentimento explícito do titular dos dados.

Neste cenário, o padrão de privacidade Obtaining Explicit Consent proporciona transparência e confiança no processo de coleta de dados pessoais, pois garante que os usuários tenham o controle total sobre o compartilhamento de suas informações pessoais. A Figura 47 destaca a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero fazer um pedido de alimentos pelo aplicativo.
Para que eu possa receber os alimentos em minha residência.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.
- Endereço.
- Telefone.
- Histórico de Pedidos.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Fornecer informações claras e objetivas sobre quais informações pessoais serão coletadas, como serão utilizadas e com quem serão compartilhadas.
- O pedido só poderá ser realizado mediante o consentimento informado pelo usuário.
- Nenhum dado pessoal dever ser coletado antes do usuário dar seu consentimento.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Obtaining Explicit Consent</td></tr>
</table>

Figura 47. História de Usuário Utilizando o Padrão de Privacidade Obtaining Explicit Consent.

Personal Data Store

Eduardo quer comprar um novo par de tênis de futsal. Ele está preocupado com a segurança e proteção de seus dados pessoais durante a compra on-line. Por isso, em vez de fornecer diretamente suas informações pessoais, ele gostaria de utilizar um serviço local de armazenamento de dados pessoais de sua confiança.

Neste contexto, o padrão de privacidade Personal Data Store pode ser utilizado, pois permite que, ao efetuar a compra do produto no *website*, Eduardo precisa apenas permitir ao sistema local compartilhar seus dados pessoais com a loja on-line. A comunicação entre o *website* e o *token* pessoal ocorre de maneira criptografada e, após a transação ser concluída, Eduardo recebe uma notificação da confirmação da compra. A Figura 48 exibe a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero fazer compras pelo aplicativo.
Para que eu possa receber o produto em minha residência.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.
- Endereço.
- Telefone.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Permitir que o usuário forneça seus dados pessoais por meio indireto ao aplicativo.
- Deve ser possível ao usuário utilizar serviços locais de armazenamento de dados pessoais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Personal Data Store.</td></tr>
</table>

Figura 48. História de Usuário Utilizando o Padrão de Privacidade Personal Data Store.

Private Link

Fábio possui uma pasta com vários documentos que ele gostaria de compartilhar com os demais diretores da organização que trabalha. No entanto, ele está preocupado com a privacidade das informações visto que algumas delas são confidenciais.

Para garantir a privacidade dos documentos compartilhados, o padrão de privacidade Private Link pode ser utilizado, pois o mesmo gera um link contendo uma

complexa *string* de caracteres aleatórios. Este link pode ser compartilhado com outros usuários que terão acesso às informações compartilhadas. A Figura 49 descreve a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um diretor.
Eu quero compartilhar relatórios da organização.
Para que outros diretores tomem conhecimento dos últimos investimentos.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Telefone.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- As informações contidas nos relatórios são confidenciais e apenas determinados perfis podem acessá-las.
- Apenas pessoas com o link correto podem acessar os arquivos.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Private Link.</td></tr>
</table>

Figura 49. História de Usuário Utilizando o Padrão de Privacidade Private Link.

Reasonable Level of Control

Mateus é um usuário de uma rede social e está preocupado com a privacidade de suas informações pessoais. Ele deseja ter um controle da visibilidade de suas informações pessoais, como por exemplo, nome completo, foto de perfil e E-mail, além de suas publicações cotidianas.

Com o intuito de preservar a privacidade dos dados pessoais dos usuários da rede social, pode-se utilizar o padrão de privacidade Reasonable Level of Control, pois garantirá que o usuário gerencie suas informações pessoais, além de manter o controle de compartilhamento com níveis específicos de visibilidade. A Figura 50 aborda a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário de rede social.
Eu quero compartilhar minhas fotografias.
Para que eu possa interagir com meus amigos.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Histórico de Publicações.</td><td>Dados Pessoais Sensíveis:
- Foto de Perfil
- Fotografias</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Fornecer ao usuário um painel de configurações de privacidade para que ele controle o nível de visibilidade de suas informações pessoais.
- Possibilitar que o usuário defina o nível de visibilidade para suas publicações e fotografias.
- Os níveis de visibilidade disponíveis são: público, apenas amigos, amigos específicos, somente o próprio usuário.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Reasonable Level of Control.</td></tr>
</table>

Figura 50. História de Usuário Utilizando o Padrão de Privacidade Reasonable Level of Control.

Reciprocity

Guilherme é um usuário frequente de um fórum de discussões sobre desenvolvimento de software. Ele gosta de compartilhar seus conhecimentos e aprender com outros membros da comunidade. Em algumas ocasiões, Guilherme verificou que outro membro do fórum tinha o perfil necessário na empresa em que trabalha, porém, a plataforma responsável pela manutenção do fórum não exibe o nome completo e e-mail de maneira pública.

Neste contexto, o padrão Reciprocity poderia ser aplicado, pois permite que usuários acessem dados pessoais de outros usuários somente se eles concordarem em compartilhar suas próprias informações pessoais. A Figura 51 destaca a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um membro de fórum de desenvolvimento de software.
Eu quero obter dados pessoais de outros membros.
Para que eu possa enviar propostas de recrutamento e seleção.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Histórico de Publicações.</td><td>Dados Pessoais Sensíveis:
- Gênero.
- Foto de Perfil.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
</table>

Restrições: - Fornecer ao usuário um painel de configurações de privacidade para que ele controle o nível de visibilidade de suas informações pessoais. - Possibilitar que o usuário visualize informações pessoais de outros usuários somente se seus dados pessoais estiverem compartilhados aos demais.
Recomendações de Padrões de Privacidade: - Reciprocity.

Figura 51. História de Usuário Utilizando o Padrão de Privacidade Reciprocity.

Selective Access Control

Ricardo é um usuário de rede social. Diariamente ele compartilha conteúdos com seus contatos, entre os conteúdos publicados por Ricardo, encontra-se assuntos esportivos, finanças, trabalho e lazer.

Para uma melhor efetividade e engajamento, Ricardo gostaria de direcionar seus conteúdos a determinados públicos, por exemplo, fotografias e momentos relacionados a diversão, compartilhar apenas com membros da família. Conteúdos sobre futebol, com amigos. Atualizações e Cursos, com colegas de trabalho.

Para este cenário, pode-se utilizar o padrão de privacidade Selective Access Control, pois permite que Ricardo selecione cuidadosamente quais amigos farão parte de cada círculo de amizade, consequentemente, a publicação postada à um determinado grupo não poderá ser acessado por pessoas de outro. A Figura 52 exibe a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário de rede social. **Eu quero** compartilhar conteúdo apenas com pessoas específicas. **Para que** eu possa melhorar a interação e engajamentos com o público alvo.		
Dados Pessoais: - Nome Completo. - E-mail. - Histórico de Publicações.	**Dados Pessoais Sensíveis:** - Gênero. - Foto de Perfil.	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Fornecer ao usuário um painel de configurações de privacidade para que ele controle os grupos de amigos. - Possibilitar adicionar e remover amigos dos grupos de amizade. - Possibilitar ao usuário, no momento da publicação, escolher qual(is) grupo(s) poderá(ão) visualizar o post.		
Recomendações de Padrões de Privacidade: - Selective Access Control.		

Figura 52. História de Usuário Utilizando o Padrão de Privacidade Selective Access Control.

Selective Disclosure

Simone está planejamento suas próximas férias e vai comprar passagens aéreas. Ao acessar o *website* da companhia aérea, ela notou que para realizar a compra é necessário ter um cadastro na plataforma, o qual coleta dados pessoais de seus clientes, como: nome completo, gênero, data de nascimento, número de cpf, número de passaporte, e-mail, telefone principal, telefone de contato e dados bancários.

Porém, Simone gostaria de realizar a compra da passagem fornecendo apenas o mínimo de dados pessoais, pois ela não tem a intenção de utilizar algumas vantagens oferecidas pela empresa, como por exemplo, programa de pontuação. Sendo Assim, o padrão Selective Disclosure pode ser utilizado neste cenário, pois ele permite que apenas os dados necessários para aquela funcionalidade específica devem ser coletados. A Figura 53 aborda a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero comprar passagens aéreas pelo website.
Para que eu possa ter comodidade e praticidade, além de poder comparar preços, horários e opções de voos disponíveis, sem precisar sair de casa ou ir até uma agência de viagens.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- CPF.
- Data de Nascimento.
- E-mail.</td><td>Dados Pessoais Sensíveis:
- Gênero.
- Dados Bancários.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Permitir que o usuário acesse de modo anônimo o itinerário dos voos.
- Permitir que o usuário realize a compra de passagens aéreas sem precisar realizar login no sistema.
- Solicitar apenas os dados necessários para a compra.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Selective Disclosure.</td></tr>
</table>

Figura 53. História de Usuário Utilizando o Padrão de Privacidade Selective Disclosure.

Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context

Leonardo gostaria de utilizar o serviço de armazenamento de arquivos na nuvem para realizar *backup* de seus arquivos pessoais. Porém, Leonardo tem receio que o provedor do serviço tenha acesso aos seus dados pessoais armazenados.

Neste caso, o padrão de privacidade Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context pode ser utilizado, pois permite que Leonardo assine um acordo com o provedor do serviço que estabeleça os termos e condições do uso de seus dados pessoais, fornecendo uma maior transparência e confiança. A Figura 54 apresenta a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero armazenar meus arquivos pessoais no servidor.
Para que eu tenha acesso a eles em qualquer lugar e a todo momento.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Informar ao usuário sobre a política de privacidade adotada pela organização, expondo os termos e condições de uso dos dados pessoais dos titulares.
- Coletar o consentimento do usuário com os termos e condições de uso de seus dados.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context.</td></tr>
</table>

Figura 54. História de Usuário Utilizando o Padrão de Privacidade Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context.

Single Point of Contact

Patrícia gostaria de fazer reclamações referentes aos produtos que adquiriu em uma loja virtual. Para isso, ela deseja acessar o *website* e falar diretamente com um atendente, mesmo não estando logada em seu perfil. Porém, Patrícia tem receio de compartilhar seus dados pessoais no chat, pois terceiros podem ter acesso às informações.

Neste cenário, o padrão de privacidade Single Point of Contact pode ser utilizado, visto que as informações fornecidas naquele canal de comunicação são criptografas e é o único ponto em que as informações são transmitidas, evitando a

divulgação dos dados para terceiros. A Figura 55 aborda a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero fazer reclamações pelo chat de mensagens instantâneas.
Para que minhas solicitações sejam atendidas de maneira rápida.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- CPF.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Informar ao usuário sobre a política de privacidade adotada pela organização, expondo os termos e condições de uso dos dados pessoais dos titulares.
- Coletar o consentimento do usuário para com os termos e condições de uso de seus dados.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Single Point of Contact.</td></tr>
</table>

Figura 55. História de Usuário Utilizando o Padrão de Privacidade Single Point of Contact.

User Data Confinement Pattern

A empresa de seguros do veículo do Heitor está implantando um novo modo de precificar o valor do veículo de seus assegurados. Além dos atributos como modelo, marca e ano do veículo, considerará a quilometragem rodada pelo veículo.

Heitor está apreensivo com isso, pois não gostaria que a empresa o monitorasse por geolocalização. Com isso, o padrão de privacidade User Data Confinement Pattern pode ser adotado neste cenário, pois a relação de confiança pode ser alterada. Em vez do provedor de serviços coletar a geolocalização para realizar o cálculo de quilometragem, o próprio veículo pode realizar o processamento das informações e enviar ao provedor apenas o resultado final do cálculo, minimizando os dados coletados de seus clientes. A Figura 56 destaca a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um sistema.
Eu quero verificar quantos quilómetros o veículo rodou no mês.
Para que eu possa calcular o valor final do seguro do cliente.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Carteira Nacional de Habilitação.
- Renavam.
- Quilometragem.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Todos os dados pessoais de geolocalização devem ficar sob posse do assegurado.
- O processamento de dados deve ocorrer no lado do cliente.
- O provedor de serviços deve receber apenas o renavam e a quilometragem rodada.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- User Data Confinement Pattern.</td></tr>
</table>

Figura 56. História de Usuário Utilizando o Padrão de Privacidade User Data Confinement Pattern.

Added-Noise Measurement Obfuscation

Anderson é cliente de uma concessionária de energia elétrica que realiza as medições do uso de eletricidade por meio de medidores inteligentes que enviam diariamente os dados de consumo de energia de cada usuário. No entanto, Anderson possui uma preocupação, pois os valores obtidos pelas medições podem revelar mais informações, como por exemplo, seus hábitos pessoais.

Para proteger a privacidade do usuário, pode-se aplicar o padrão de Added-Noise Measurement Obfuscation nesta funcionalidade, adicionando ruído aos dados coletados, tornando-os menos precisos, mas ainda úteis para fins de monitoramento. A Figura 57 exibe a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um sistema.
Eu quero obter os dados das medições do uso de eletricidade.
Para que eu possa calcular o valor total da fatura de cada cliente.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Identificador da Residência.
- Consumo Quilowatt Hora.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
</table>

Restrições: - Adicionar valores de ruído antes de transmitir ao provedor de serviços de modo a ofuscar os dados reais.
Recomendações de Padrões de Privacidade: - Added-Noise Measurement Obfuscation.

Figura 57. História de Usuário Utilizando o Padrão de Privacidade Added-Noise Measurement Obfuscation.

Aggregation Gateway

Carla utiliza um *smartwatch* que coleta constantemente seus dados pessoais a fim de monitorar sua saúde. Em seu relógio ela possui um aplicativo que utiliza destes dados para monitorar seu progresso e fornecer orientações e lembretes para a prática de exercícios físicos.

Com o intuito de incentivar os usuários do aplicativo, diariamente são mostrados relatórios comparando os números de Carla com os demais usuários, o que gera uma apreensão em Carla, pois os dados pessoais de todos os usuários estão sendo coletados e transmitidos ao provedor de serviço.

Neste contexto, o padrão de privacidade Aggregation Gateway pode ser aplicado, pois este visa anonimizar e criptografar todos os dados pessoais, antes mesmo de serem transmitidos ao provedor de serviço. Ao receber os dados, o provedor terá posse apenas dos dados agregados, sem comprometer a privacidade e segurança dos titulares dos dados. A Figura 58 destaca a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário. **Eu quero** compartilhar meus dados de saúde. **Para que** eu possa monitorar meu progresso e obter orientações de exercícios.		
Dados Pessoais: - Nome Completo.	**Dados Pessoais Sensíveis:** - Gênero. - Frequência Cardíaca. - Qualidade do Sono. - Quantidade de Passos. - Calorias Gastas. - Minutos de Atividades Físicas.	**Tempo de Retenção:** 20 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). - Lei nº 13.787 - Sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.		

Restrições: - Os dados coletados devem ser anonimizados e criptografados antes de realizar o envio ao provedor de serviço. - Os dados de todos os usuários devem estar agregados impossibilitando a identificação e garantindo a privacidade e segurança de cada usuário.
Recomendações de Padrões de Privacidade: - Aggregation Gateway.

Figura 58. História de Usuário Utilizando o Padrão de Privacidade Aggregation Gateway.

Trustworthy Privacy Plug-in

Carlos utiliza um aplicativo de mensagens instantâneas para interagir com seus amigos e familiares. Porém, Carlos está preocupado com sua privacidade, pois as mensagens enviadas por ele são recebidas primeiramente pelo provedor de serviço que as encaminha para o cliente destino. Com isso, terceiros poderiam ter acesso a informações pessoais e confidenciais enviadas e/ou recebida por ele.

Neste contexto, o padrão de privacidade Trustworthy Privacy Plug-in pode auxiliar na arquitetura do aplicativo, pois um *plugin* pode ser adicionado ao aplicativo de mensagem instantânea para que o texto seja criptografado antes de ser enviado ao provedor de serviço e descriptografado apenas no dispositivo do destinatário. A Figura 59 descreve a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** enviar mensagens criptografadas aos meus contatos. **Para que** apenas o destinatário consiga ter acesso a elas.		
Dados Pessoais: - Nome Completo. - Telefone. - Mensagem de Texto.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Criptografar as mensagens antes de serem enviadas ao provedor de serviço. - Descriptografar as mensagens ao serem recebidas pelo destinatário.		
Recomendações de Padrões de Privacidade: - Trustworthy Privacy Plug-in.		

Figura 59. História de Usuário Utilizando o Padrão de Privacidade Trustworthy Privacy Plug-in.

Anonymity Set

Fernando é usuário de uma plataforma de compartilhamento de arquivos. Porém, preocupado com sua privacidade, ele gostaria de compartilhar arquivos de modo que sua identidade não pudesse ser revelada. Neste cenário, o padrão de privacidade Anonymity Set pode ser utilizado, pois permite que indivíduos realizem transações, ações ou comunicações sem que sua identidade seja descoberta. A Figura 60 destaca a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero compartilhar arquivos com outros usuários sem revelar minha identidade.
Para que outros usuários possam utilizar os arquivos para o próprio entretenimento.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O link de compartilhamento gerado deve ser exclusivo.
- O link de compartilhamento deve acessar apenas os arquivos compartilhados e não pode estar vinculado a identidade real do remetente.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Anonymity Set.</td></tr>
</table>

Figura 60. História de Usuário Utilizando o Padrão de Privacidade Anonymity Set.

Anonymous Reputation-based Blacklisting

Bruna realizou compras em uma loja virtual e, ao receber os produtos adquiridos, Bruna quer avaliar os vendedores, porém quer manter sua identidade em sigilo. Por outro lado, a loja virtual precisa considerar o perfil do usuário que está avaliando o vendedor, pois um usuário mal-intencionado pode realizar inúmeras avaliações a um determinado vendedor apenas para prejudica-lo.

Neste cenário, o padrão de privacidade Anonymous Reputation-based Blacklisting pode ser utilizado. O sistema deve vincular valores da reputação a uma sessão e mantém uma lista de sessões ofensivas. Desta maneira, quando o mesmo usuário anônimo retornar a plataforma, haverá um histórico a ser considerado, mesmo que a identidade do usuário não seja conhecida. A Figura 61 apresenta a história de usuário para o contexto mencionado.

História de Usuário		
Como um comprador. **Eu quero** avaliar, de maneira anônima, os vendedores de produtos adquiridos. **Para que** minha privacidade seja preservada.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Fornecer aos usuários credenciais para autenticação anônima. - Registrar um valor de reputação para cada sessão. - Os valores de reputação devem estar vinculados a sessão e não ao usuário. - Manter uma lista de sessões ofensivas a fim de impedir que um usuário mal-intencionado realize avaliações de vendedores.		
Recomendações de Padrões de Privacidade: - Anonymous Reputation-based Blacklisting.		

Figura 61. História de Usuário Utilizando o Padrão de Privacidade Anonymous Reputation-based Blacklisting.

Onion Routing

Paulo é usuário de aplicativo de mensagens instantâneas, porém está preocupado com sua privacidade e gostaria de enviar mensagens de maneira completamente anônima para outros usuários do mesmo aplicativo.

Para manter sua identidade anônima e proteger as mensagens de acesso de terceiros durante a comunicação, pode-se utilizar o padrão de privacidade Onion Routing, que visa adicionar camadas de criptografias para proteger a identidade do remetente. A Figura 62 destaca a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** mensagens de maneira anônima para outros usuários. **Para que** minha identidade e mensagens permaneçam protegidas e confidenciais durante a comunicação.		
Dados Pessoais: - Mensagens de Texto.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Criptografar as mensagens antes de serem enviadas ao destinatário. - Cada nó da comunicação só pode conhecer seu sucessor e predecessor.		
Recomendações de Padrões de Privacidade: - Onion Routing.		

Figura 62. História de Usuário Utilizando o Padrão de Privacidade Onion Routing.

Pseudonymous Identity

Marcos gostaria de diversificar seus investimentos financeiros. Para isso, gostaria de comprar e vender criptomoedas em uma Exchange. No entanto, Marcos está preocupado com sua privacidade e gostaria de realizar as transações de compra e venda de criptomoedas sem relevar seus dados pessoais.

Neste cenário, o padrão de privacidade Pseudonymous Identity pode ser utilizado, pois possibilita aos usuários do sistema utilizar-se de pseudônimos em vez de informações de identificação pessoal. A Figura 63 descreve a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero realizar compra de criptomoedas utilizando pseudônimos.
Para que eu possa garantir a privacidade e a segurança das minhas transações financeiras.</td></tr>
<tr><td>Dados Pessoais:
- Valor a ser negociado.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Criar um pseudônimo ao usuário o qual será utilizado para realizar a transação financeira.
- Toda e qualquer movimentação financeira do usuário, deve-se utilizar o pseudônimo do mesmo.
- A realização de transações financeiras utilizando o pseudônimo deve ser opcional e configurável pelo usuário.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Pseudonymous Identity.</td></tr>
</table>

Figura 63. História de Usuário Utilizando o Padrão de Privacidade Pseudonymous Identity.

Pseudonymous Messaging

Camila é uma ativista política e gostaria de criar um grupo no aplicativo de mensagens instantâneas de pessoas que possuem a mesma orientação política que ela para discutirem sobre o tema. Porém, como este grupo tem o objetivo de tratar de assuntos delicados, Camila gostaria de enviar mensagens utilizando um pseudônimo para que sua identidade verdadeira fosse preservada.

Sendo assim, o padrão de privacidade Pseudonymous Messaging pode ser utilizado, pois permite que usuários interajam entre si sem revelar sua identidade real. A Figura 64 apresenta a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ter a opção de enviar mensagens utilizando um pseudônimo para outros usuários.
Para que eu possa manter minha privacidade e segurança online.</td></tr>
<tr><td>Dados Pessoais:
- Mensagem de Texto.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Criar um pseudônimo ao usuário o qual poderá ser utilizado para interagir com outros usuários.
- A funcionalidade de envio de mensagens pseudônimas deve ser opcional e configurável pelo usuário.
- O pseudônimo do remetente deve ser exibido claramente aos destinatários, para que saibam que estão recebendo uma mensagem pseudônima.
- Os usuários devem ter a opção de bloquear ou denunciar usuários que enviam mensagens pseudônimas inapropriadas ou prejudiciais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Pseudonymous Messaging.</td></tr>
</table>

Figura 64. História de Usuário Utilizando o Padrão de Privacidade Pseudonymous Messaging.

Use of Dummies

Michele faz publicações diariamente em seu perfil em uma rede social. Entretanto, ela notou que em todas as suas publicações a plataforma realiza coleta de dados de geolocalização para exibir os locais em que as fotografias foram registradas.

Apesar de Michele ter consentido com a coleta desses dados, em determinados *posts* ela não gostaria que a plataforma utilizasse os dados de localização de seu dispositivo. Deste modo, o padrão de privacidade Use of Dummies pode ser utilizado para que os dados reais de geolocalização dos usuários sejam alterados por dados fictícios, preservando a privacidade de dados dos usuários da plataforma. A Figura 65 destaca a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ter a opção de fornecer informações fictícias de geolocalização.
Para que eu possa manter minha localização real em sigilo, mas ainda assim obter informações úteis com base em uma localização aproximada.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:
- Foto de Perfil.
- Fotografias.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O uso de informações fictícias deve ser opcional e o usuário pode optar por fornecer sua localização real, se desejar.
- O aplicativo irá fornecer opções para os usuários selecionarem um local fictício com base em uma lista de locais comuns (como cafeterias, parques, shopping centers, etc.).
- O aplicativo deve permitir que os usuários insiram manualmente informações fictícias, como cidade ou código postal, para obter informações úteis com base em uma localização aproximada.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Use of Dummies.</td></tr>
</table>

Figura 65. História de Usuário Utilizando o Padrão de Privacidade Use of Dummies.

Attribute Based Credentials

Miguel possui um *smartwatch* o qual faz uso regularmente. Neste dispositivo há um aplicativo que armazena todos os dados coletados referentes a sua saúde. Além disso, há diferentes perfis de usuários, como por exemplo, paciente, médicos e outros profissionais de saúde.

O perfil paciente, como é o caso de Miguel, apenas tem acesso aos seus próprios dados de saúde. Por outro lado, médicos e demais profissionais de saúde podem receber os dados pessoais de seus pacientes. Neste cenário, Miguel compreende a importância de seus médicos terem acesso ao histórico de todos os seus dados de saúde, porém, gostaria de selecionar quais dados pessoais serão compartilhados com cada médico, preservando ao máximo sua privacidade. Para este cenário, o padrão de privacidade Attribute Based Credentials pode ser aplicado. A Figura 66 exibe a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um paciente.
Eu quero ser capaz de escolher quais dados de saúde compartilhar com cada médico.
Para que eu possa garantir a privacidade dos meus dados pessoais.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.
- Endereço.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:
- Gênero.
- Altura.
- Peso.
- Frequência Cardíaca.
- Qualidade do Sono.</td><td>Tempo de Retenção:
20 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 13.787 - Sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.</td></tr>
<tr><td colspan="3">Restrições:
- O sistema deve ser capaz de armazenar e gerenciar as credenciais de atributos dos usuários de forma segura e privada.
- Os usuários devem ter controle total sobre quais informações específicas eles compartilham e com que profissional.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Attribute Based Credentials.</td></tr>
</table>

Figura 66. História de Usuário Utilizando o Padrão de Privacidade Attribute Based Credentials.

Protection Against Tracking

Helena é cliente de uma loja virtual, recentemente ela acessou este *e-commerce* e realizou uma busca por um produto que está desejando adquiri-lo, porém ainda não finalizou a compra. A partir deste dia, Helena está recebendo diariamente em seu E-mail e em suas redes sociais propagandas do produto pesquisado, o que a tem deixado insegura em relação aos seus dados pessoais que foram coletados pela plataforma.

Neste contexto, o padrão de privacidade Protection Against Tracking pode ser utilizado para restringir o uso de *cookies* do lado do cliente para que os dados de navegação não sejam coletados. A Figura 67 descreve a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ter a opção de desativar o rastreamento de navegação na loja virtual.
Para que minhas informações pessoais não sejam coletadas e compartilhadas com terceiros sem meu consentimento.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Endereço IP.
- Navegador.
- Histórico de Navegação.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
</table>

Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Restrições: - Possibilitar ao usuário desabilitar o rastreamento da sua navegação pelo website. - Explicar os efeitos da desativação do rastreamento, como a impossibilidade de receber ofertas personalizadas pelo usuário. - Prover ao usuário a opção de habilitar o rastreamento de sua navegação. Para isto, informações do que será coletado, para que fim e com quem os dados serão compartilhados devem ser exibidos. O rastreamento só poderá ser habilitado após coletar o consentimento do usuário.
Recomendações de Padrões de Privacidade: - Protection Against Tracking.

Figura 67. História de Usuário Utilizando o Padrão de Privacidade Protection Against Tracking.

Strip Invisible Metadata

Bruno é jornalista e fotógrafo em um jornal de sua cidade. Ao apurar as notícias, ele armazena todos os documentos, inclusive fotografias, no ambiente interno da empresa o qual outros colaboradores tem acesso.

Muitos destes documentos e fotografias são utilizados nos jornais físicos e virtuais produzidos pela empresa. Bruno, preocupado com os metadados presentes nos documentos e fotografias produzidos por ele, gostaria que o próprio sistema utilizado pela organização remova toda e qualquer informação contida nos arquivos a fim de preservar a identidade da fonte jornalística.

Para este cenário, o padrão Strip Invisible Metadata pode ser utilizado, visto que seu objetivo é excluir metadados invisíveis que podem conter informações pessoais ou confidenciais, como localização, informações do dispositivo, software e outros dados que possam ser usadas para identificar ou rastrear um usuário sem o seu conhecimento ou consentimento. A Figura 68 aborda a história de usuário para o exemplo citado.

História de Usuário		
Como um jornalista. **Eu quero** ter a capacidade de remover todos os metadados invisíveis de um arquivo. **Para que** a privacidade e segurança da minha fonte jornalística seja preservada.		
Dados Pessoais: - Arquivos. - Documentos. - Fotografias.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		

Restrições: - O sistema deve permitir que o jornalista selecione vários arquivos para a remoção de metadados invisíveis. - O sistema deve apresentar um resumo dos metadados que serão removidos antes da ação de remoção. - O sistema deve remover todos os metadados invisíveis do arquivo selecionado e salvar a novo arquivo sem eles. - O sistema deve manter os metadados visíveis, como data de criação, nome do arquivo e tamanho do arquivo.
Recomendações de Padrões de Privacidade: - Strip Invisible Metadata.

Figura 68. História de Usuário Utilizando o Padrão de Privacidade Strip Invisible Metadata.

Abridged Terms and Conditions

Lucas em suas horas vagas gosta de jogar games virtuais. Recentemente ele instalou um game de corrida de carros, porém, ao abrir o aplicativo, notou que o mesmo solicitou dados pessoais para realizar seu cadastro sem ao menos exibir os termos e condições de uso do game. Lucas então resolveu procurar nas opções do aplicativo os termos e condições, ao encontra-lo, notou que os desenvolvedores do game utilizaram uma linguagem de difícil compreensão, com jargões jurídicos e técnicos, o que dificultou o entendimento do documento.

Nesta situação, o padrão de privacidade Abridged Terms and Conditions pode ser implementado, pois visa apresentar os termos e condições de uso de aplicativos de forma clara e concisa para ser compreendido facilmente pelos usuários. A Figura 69 destaca a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** que os termos e condições de uso sejam apresentados de forma clara e concisa. **Para que** eu possa entender facilmente quais são meus direitos e responsabilidades ao usar o aplicativo.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Ao iniciar o aplicativo pela primeira vez, o usuário deverá ser apresentado a uma tela com uma versão resumida dos termos e condições de uso. - Os termos e condições serão escritos de forma clara e concisa, utilizando linguagem simples e evitando jargões jurídicos e técnicos que possam dificultar a compreensão. - O usuário poderá acessar a versão completa dos termos e condições de uso a qualquer momento por meio de um link. - Quando houver alguma atualização nos termos e condições de uso, o usuário será notificado e deverá concordar novamente com os termos antes de continuar usando o aplicativo.		
Recomendações de Padrões de Privacidade: - Abridged Terms and Conditions.		

Figura 69. História de Usuário Utilizando o Padrão de Privacidade Abridged Terms and Conditions.

Appropriate Privacy Icons

Rafaela frequentemente faz publicações sobre seu cotidiano no seu perfil na rede social. Porém, ela notou que usuários desconhecidos estavam curtindo e comentando suas publicações, pois as publicações estavam definidas com visibilidade "pública", ou seja, todos os usuários da rede social possuíam acesso aos *posts* de Rafaela. Isso ocorreu devido as publicações não ilustrarem de maneira clara qual era a visibilidade configurada.

Para solucionar este problema, o padrão de privacidade Appropriate Privacy Icons pode ser utilizado, pois estabelece o uso de ícones claros e facilmente reconhecíveis que informam aos usuários sobre as configurações de privacidade de cada postagem. Por exemplo, uma postagem pode ter um ícone de cadeado para indicar que está visível apenas para o próprio autor, enquanto outra postagem pode ter um ícone de globo para indicar que é pública e visível para qualquer pessoa. A Figura 70 exibe a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário de rede social.
Eu quero visualizar ícones de privacidade adequados em cada publicação realizada na rede social.
Para que eu consiga identificar de maneira clara e objetiva qual o nível de visibilidade contém aquela publicação.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Os ícones de privacidade devem ser claramente visíveis e fáceis de compreender.
- Os ícones devem ser consistentes com os padrões de privacidade estabelecidos na indústria.
- O usuário deve ser capaz de clicar nos ícones para obter mais informações sobre a visibilidade da publicação.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Appropriate Privacy Icons.</td></tr>
</table>

Figura 70. História de Usuário Utilizando o Padrão de Privacidade Appropriate Privacy Icons.

Ambient Notice

Adriana possui em seu aparelho celular um aplicativo de previsão do tempo. Quando o aplicativo foi instalado, ela concedeu permissão para que houvesse a coleta de dados de geolocalização, que é utilizado para que o sistema consiga informar com exatidão ao usuário a previsão do tempo para o local em que se encontra.

Entretanto, a fim de preservar sua privacidade, Adriana gostaria de ser informada quando o aplicativo de previsão do tempo realiza a coleta de dados de geolocalização. Deste modo, o padrão de privacidade Ambient Notice pode ser utilizado, notificando o usuário no momento em que a coleta de dados pessoais ocorrer. A Figura 71 aborda a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero receber notificações sobre as condições climáticas na minha região.
Para que eu possa me manter informado sobre possíveis mudanças climáticas.</td></tr>
<tr><td>Dados Pessoais:
- Geolocalização.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O aplicativo não deve coletar dados adicionais de geolocalização sem o consentimento explícito do usuário.
- O aplicativo deve exibir uma notificação quando a coleta de dados de geolocalização é ativada.
- O aplicativo deve permitir que o usuário desative a coleta de dados de geolocalização a qualquer momento nas configurações.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Ambient Notice.</td></tr>
</table>

Figura 71. História de Usuário Utilizando o Padrão de Privacidade Ambient Notice.

Appropriate Privacy Feedback

Luiz é usuário de um aplicativo de treinos físicos. Ao instalar o sistema, ele fez a leitura e concordou com os termos e condições de uso. Porém, após alguns meses de uso do aplicativo, Luiz gostaria de sugerir algumas modificações nas condições de uso dos dados pessoais dos usuários. Entretanto, o aplicativo não possui um canal de coleta de *feedback* relacionado as informações pessoais.

Sendo assim, o padrão de privacidade Appropriate Privacy Feedback poderia ser aplicado a este caso, garantindo uma maior transparência do uso e compartilhamento dos dados dos titulares, além de permitir aos usuários compartilharem suas preocupações, opiniões e sugestões sobre as práticas de privacidade que precisam ser melhoradas. A Figura 72 apresenta a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** fornecer feedback sobre a forma como meus dados estão sendo processados e compartilhados. **Para que** eu possa ter confiança de que minha privacidade está sendo respeitada.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - A funcionalidade deve ser claramente visível e de fácil acesso para o usuário. - A funcionalidade deve permitir que o usuário forneça feedback de forma anônima, se assim desejar. - O feedback fornecido pelo usuário deve ser coletado e avaliado para melhorar as práticas de privacidade do aplicativo.		
Recomendações de Padrões de Privacidade: - Appropriate Privacy Feedback.		

Figura 72. História de Usuário Utilizando o Padrão de Privacidade Appropriate Privacy Feedback.

Asynchronous Notice

Juliana é cliente de um determinado banco. Para sua maior comodidade, Juliana realiza todas as suas transações financeiras por meio do aplicativo do próprio banco.

Ao instalar o aplicativo, Juliana leu atentamente e consentiu com os termos e condições de uso. A cada nova atualização do aplicativo, Juliana lê novamente os termos e condições para se certificar que o banco não os alterou, porém isso demanda tempo e, na maioria das vezes, ela constata que não houve alterações significativas.

Neste cenário, o padrão de privacidade Asynchronous Notice poderia ser utilizado na solução, pois o aplicativo notificaria seus usuários apenas se alguma alteração ocorrer nos termos e condições de uso, permitindo a eles se concordam ou não com as novas condições por meio de um novo consentimento informado. A Figura 73 aborda a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário. **Eu quero** ser notificado sobre quaisquer mudanças na política de privacidade. **Para que** eu possa estar ciente das informações que estão sendo coletadas e como elas estão sendo usadas.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		

Restrições: - A notificação deve ser claramente visível para o usuário. - A notificação deve fornecer informações claras e detalhadas sobre quaisquer mudanças na política de privacidade. - A notificação deve permitir que o usuário aceite ou rejeite as mudanças na política de privacidade.
Recomendações de Padrões de Privacidade: - Asynchronous Notice.

Figura 73. História de Usuário Utilizando o Padrão de Privacidade Asynchronous Notice.

Awareness Feed

Márcia é uma nova usuária de rede social. Recentemente ela criou um perfil por indicações de amigas e familiares, porém, ainda não está familiarizada com a plataforma e com os riscos referentes a privacidade de seus dados pessoais.

Neste contexto, o padrão de privacidade Awareness Feed pode auxiliar os usuários (novos ou não) da plataforma, mostrando um *feed* de conscientização capaz de informar as práticas e políticas de privacidade e segurança, desta maneira, os usuários receberão informações detalhadas que os auxiliarão nas configurações de privacidade pessoal. A Figura 74 destaca a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** ter acesso a um feed de conscientização para me manter informado sobre as práticas de privacidade e segurança da plataforma. **Para que** eu possa tomar melhores decisões informadas sobre o uso da plataforma.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - O feed de conscientização deve estar disponível na página inicial do aplicativo. - O feed de conscientização deve incluir informações sobre quaisquer mudanças na política de privacidade e segurança da plataforma. - O feed de conscientização deve ser atualizado regularmente e os usuários devem ser notificados sobre novas postagens.		
Recomendações de Padrões de Privacidade: - Awareness Feed.		

Figura 74. História de Usuário Utilizando o Padrão de Privacidade Awareness Feed.

Data Breach Notification Pattern

Gabriel é usuário de uma rede social. Recentemente, Gabriel leu em portais de notícias e noticiários na TV que a rede social concorrente a que ele utiliza, teve os dados de usuários vazados por uma falha de segurança. Ao tomar conhecimento do fato, Gabriel ficou apreensivo, visto que a rede social que ele utiliza poderia também ter sofrido ataques semelhantes e escondeu de seus usuários.

Desse modo, o padrão de privacidade Data Breach Notification Pattern cita que a confiança do usuário pode ser fortalecida mesmo ao detectar uma violação de dados. Para isto, deve-se notificar as autoridades e titulares de dados, além de mitigar os riscos. A Figura 75 exibe a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ser notificado imediatamente se houver uma violação de dados.
Para que eu possa tomar medidas para proteger minhas informações pessoais.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Os usuários devem ser notificados imediatamente após a detecção da violação.
- A notificação deve incluir informações sobre os dados pessoais que foram comprometidos.
- Os usuários devem ser orientados com instruções claras sobre como proteger suas informações pessoais.
- Os usuários devem receber informações sobre as medidas que o serviço está tomando para corrigir a violação e evitar violações futuras.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Data Breach Notification Pattern.</td></tr>
</table>

Figura 75. História de Usuário Utilizando o Padrão de Privacidade Data Breach Notification Pattern.

Privacy Aware Wording

Recentemente, Daniel instalou um aplicativo de *delivery* de alimentos o qual coleta seus dados pessoais para oferecer promoções e sugestões baseados em sua geolocalização e preferências.

Ao acessar o aplicativo pela primeira vez, foi apresentado ao Daniel os termos de serviço e política de privacidade. Entretanto, o texto continha termos técnicos e jurídicos de difícil compreensão. Sendo assim, Daniel gostaria que o documento fosse

escrito de forma clara e objetiva, de fácil compreensão para que ele consiga tomar as melhores decisões em relação a proteção e segurança de seus dados pessoais.

Neste caso, o padrão Privacy Aware Wording pode auxilia-lo, pois menciona que os termos e condições de uso dos sistemas devem ser escritos utilizando vocabulário de fácil compreensão por parte dos usuários. A Figura 76 destaca a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero que os termos de serviço e política de privacidade sejam apresentados de forma clara e de fácil compreensão.
Para que eu possa tomar uma decisão informada sobre o uso da plataforma.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- A apresentação dos termos de serviço e política de privacidade deve seguir as leis e regulamentações aplicáveis.
- Os termos de serviço e política de privacidade devem ser apresentados de forma clara e objetiva, evitando termos técnicos ou jurídicos excessivos.
- Os usuários devem ler os termos de serviço e política de privacidade antes de concordar com eles.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Aware Wording.</td></tr>
</table>

Figura 76. História de Usuário Utilizando o Padrão de Privacidade Privacy Aware Wording.

Dynamic Privacy Policy Display

Marcelo faz suas compras por meio de um aplicativo de comércio eletrônico. Para oferecer melhores ofertas e promoções, o aplicativo realiza coleta de dados de seus usuários mediante consentimento informado que é coletado no primeiro acesso.

No entanto, o aplicativo constantemente realiza alterações em sua política de privacidade, muitas vezes isso ocorre para se manter em conformidade com as leis e regulamentos vigentes. Marcelo, preocupado com a privacidade de seus dados pessoais, gostaria de receber uma notificação de maneira objetiva e concisa sempre que ocorrerem atualizações na política de privacidade do aplicativo. Neste contexto, o padrão de privacidade Dynamic Privacy Policy Display pode ser aplicado. A Figura 77 descreve a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** ser notificado sempre que houver alterações na política de privacidade do aplicativo. **Para que** eu possa compreender como meus dados estão sendo coletados, processados e compartilhados.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - O aplicativo deve exibir uma notificação objetiva e visível quando houver mudanças na política de privacidade. - A notificação deve informar o usuário sobre o que foi alterado na política de privacidade. - Ao clicar na notificação, o usuário deve ser direcionado para a nova política de privacidade. - Caso o usuário não aceite as alterações na política de privacidade, ele deve ser capaz de encerrar a utilização do aplicativo.		
Recomendações de Padrões de Privacidade: - Dynamic Privacy Policy Display.		

Figura 77. História de Usuário Utilizando o Padrão de Privacidade Dynamic Privacy Policy Display.

Privacy Icons

Júlia possui um *smartwatch* que monitora diariamente suas atividades físicas. Apesar de Júlia ter lido a política de privacidade do aplicativo, por se tratar de um documento extenso e com linguagem de difícil compreensão, ela não se deu conta que, além de coletar os dados pessoais dos usuários, o provedor de serviço os compartilha com terceiros.

A fim de facilitar a compreensão do usuário em relação a coleta, processamento, armazenamento e compartilhamento de seus dados pessoais, o padrão de privacidade Privacy Icons poderia ser utilizado para incluir ícones padronizados de privacidade no documento de política de privacidade do aplicativo. A Figura 78 destaca a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário. **Eu quero** que ícones padronizados de privacidade estejam visíveis. **Para que** eu possa compreender facilmente como meus dados estão sendo coletados, como serão processados e se serão compartilhados com terceiros.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**

Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Restrições: - Os ícones de privacidade relevantes devem ser exibidos claramente e em um local visível para o usuário. - Os usuários devem poder clicar em cada ícone para obter mais informações sobre a respectiva política de privacidade.
Recomendações de Padrões de Privacidade: - Privacy Icons.

Figura 78. História de Usuário Utilizando o Padrão de Privacidade Privacy Icons.

Icons for Privacy Policies

Letícia não possui veículo pessoal e, para se locomover de um lugar a outro, gostaria de utilizar um aplicativo de transporte privado urbano. Para utilizar o aplicativo recém instalado, é necessário que Letícia faça um cadastro com seus dados pessoais, leia atentamente a política de privacidade de aplicativo e conceda seu consentimento explícito que está de acordo com os termos de utilização do aplicativo. Porém, ao tomar conhecimento do documento de política de privacidade, Letícia não conseguiu o compreender, pois, além de ser um documento extenso, faz uso de termos técnicos e jurídicos.

Um modo de simplificar a transmissão dessas informações, como por exemplo, compartilhamento de dados com terceiros, é a utilização de ícones para a política de privacidade, conforme cita o padrão de privacidade Icons for Privacy Policies. Desta maneira, o usuário, por meio de ícones, pode compreender quais dados são coletados, como ocorre o processamento e se seus dados são compartilhados com terceiros. Caso queira obter informações detalhadas, pode então ler na íntegra o documento de política de privacidade. A Figura 79 apresenta a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** compreender de maneira fácil a política de privacidade do aplicativo. **Para que** eu possa tomar decisões informadas sobre quais dados são coletados, processados, armazenados e compartilhados.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		

Restrições: - Os ícones devem ser objetivos e de fácil compreensão do seu significado. - Os ícones devem ser atualizados quando a política de privacidade sofrerem alterações. - A partir dos ícones, os usuários que desejarem informações mais detalhadas devem ter acesso direto à política de privacidade completa.
Recomendações de Padrões de Privacidade: - Icons for Privacy Policies.

Figura 79. História de Usuário Utilizando o Padrão de Privacidade Icons for Privacy Policies.

Layered Policy Design

Luciana utiliza um aplicativo de compras online. Porém, ao tentar ler a política de privacidade do *website* enfrentou dificuldades, pois o documento é extenso e desorganizado.

A fim de facilitar a compreensão, Luciana gostaria que o documento fosse organizado em camadas. Em um primeiro momento informações gerais seriam apresentadas e informações específicas e detalhadas poderiam ser acessadas em camadas subsequentes, conforme define o padrão de privacidade Layered Policy Design. A Figura 80 destaca a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** visualizar a política de privacidade de forma simplificada e organizada. **Para que** eu possa compreender melhor como meus dados pessoais são coletados, utilizados e protegidos.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - O aplicativo deve apresentar a política de privacidade em camadas, com uma visão geral na primeira camada e informações mais detalhadas em camadas subsequentes. - O usuário deve ter a opção de expandir ou contrair cada camada para visualizar mais ou menos detalhes. - Cada camada deve ser identificada por um título e ícone apropriado, para facilitar a navegação e compreensão.		
Recomendações de Padrões de Privacidade: - Layered Policy Design.		

Figura 80. História de Usuário Utilizando o Padrão de Privacidade Layered Policy Design.

Privacy Labels

Felipe utiliza um aplicativo para se conectar com seus amigos em uma rede social. Ele compreende que a rede social apresenta um risco aos seus dados pessoais, por isso é necessário ler a política de privacidade com atenção e compreender como seus dados pessoais serão coletados, armazenados, processados e compartilhados.

Porém, ao acessar o documento de política de privacidade, Felipe não conseguiu compreender todas as informações, pois o documento é extenso e desorganizado. Neste contexto, Felipe gostaria de obter um documento contendo etiquetas de privacidade que identificassem as informações, como por exemplo, descrição, finalidade de uso, retenção de dados, compartilhamento com terceiros, entre outros. Para este anseio de Felipe, pode-se utilizar o padrão de privacidade Privacy Labels. A Figura 81 descreve a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero visualizar a política de privacidade organizada com etiquetas de privacidade.
Para que eu possa compreender rapidamente como meus dados pessoais são coletados, qual a finalidade de uso, como serão retidos e com quem serão compartilhados.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O aplicativo deve apresentar a política de privacidade organizada em etiquetas de privacidade.
- No início do documento, deve haver uma legenda identificando as etiquetas de privacidade existentes.
- Cada camada deve ser identificada por um título e cor, que devem ser únicos e padronizados em todo o documento de política de privacidade.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Labels.</td></tr>
</table>

Figura 81. História de Usuário Utilizando o Padrão de Privacidade Privacy Labels.

Privacy Policy Display

Vanessa instalou um aplicativo de transporte privado urbano. Ao abrir o aplicativo pela primeira vez, ela recebeu um aviso que só poderia prosseguir mediante a leitura e obtenção de consentimento à política de privacidade do sistema. Porém, após o segundo uso do aplicativo, a política de privacidade não foi mais exibida.

Vanessa, preocupada com a privacidade de seus dados pessoais tentou encontrar o documento da política de privacidade, entretanto, não obteve sucesso.

Neste caso, o padrão de privacidade Privacy Policy Display menciona que a política de privacidade deve ser exibida não apenas na primeira vez que o aplicativo for utilizado pelo usuário, mas sim durante todo o uso do aplicativo deve haver um ícone de fácil acesso que permite ao usuário obter a política de privacidade atualizada, caso o mesmo queira revisá-la. Se os termos de uso do sistema forem atualizados, o usuário deve ser alertado sobre as alterações ocorridas para que realizem novamente a leitura e aceitem a nova política de privacidade do aplicativo. A Figura 82 apresenta a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero acessar a política de privacidade do aplicativo de modo simplificado.
Para que eu possa revisar as atualizações implementadas pela empresa.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Ao iniciar o aplicativo pela primeira vez, uma tela de política de privacidade deve ser exibida, informando os tipos de dados coletados e como eles serão usados.
- A política de privacidade deve ser facilmente acessível a partir de qualquer tela do aplicativo, por meio de um ícone ou link na barra de navegação.
- A política de privacidade deve ser clara e de fácil compreensão para o usuário, sem termos técnicos ou ambíguos.
- O usuário deve ser capaz de aceitar ou recusar a política de privacidade antes de prosseguir para o uso do aplicativo. Se o usuário recusar, o aplicativo deve ser fechado.
- Qualquer alteração na política de privacidade deve ser exibida em destaque na tela inicial do aplicativo e o usuário deve ser solicitado a revisar e aceitar novamente.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Policy Display.</td></tr>
</table>

Figura 82. História de Usuário Utilizando o Padrão de Privacidade Privacy Policy Display.

Impactful Information and Feedback

Emanoel é usuário de um aplicativo que faz a comparação de preços de produtos em diferentes *e-commerce*. Para uma melhor experiência dos usuários, o aplicativo realiza a coleta de dados pessoais e compartilha com empresas parceiras mediante consentimento informado por parte dos titulares de dados.

Ao ler a política de privacidade do aplicativo, Emanoel teve inúmeras dúvidas de quais termos e condições consentir e quais recusar. Para auxiliar usuários na

configuração do nível de privacidade de seus dados pessoais, Emanoel gostaria que o aplicativo apresentasse, por meio de informações claras e objetivas, além de gráficos e ilustrações relevantes, quais são as configurações de privacidade mais utilizadas por outros usuários.

Desta maneira, Emanoel pode se basear na configuração da maioria dos usuários, minimizando as chances de expor demasiadamente seus dados pessoais. Neste cenário, o padrão de privacidade Impactful Information and Feedback pode ser utilizado. A Figura 83 destaca a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ser informado de maneira clara e objetiva sobre as configurações de privacidade de outros usuários.
Para que eu possa tomar decisões informadas sobre a privacidade de meus dados pessoais baseadas em dados gerais de outros usuários.</td></tr>
<tr><td>Dados Pessoais:
- Preferências de Privacidade.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- As informações sobre a coleta de dados devem ser apresentadas de maneira clara e objetiva.
- As informações mais importantes devem ser destacadas.
- Os dados de configurações de outros usuários deverão ser apresentados de modo agregado, não sendo possível visualizar uma configuração de um usuário específico.
- Possibilitar ao usuário compartilhar os dados de sua configuração de privacidade, porém, isso só poderá ocorrer mediante o consentimento informado pelo usuário.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Impactful Information and Feedback.</td></tr>
</table>

Figura 83. História de Usuário Utilizando o Padrão de Privacidade Impactful Information and Feedback.

Platform for Privacy Preferences

André utiliza a internet para realizar suas atividades profissionais e pessoais. Ele notou que as políticas de privacidade dos sites que acessa são semelhantes entre si. Sendo que uma vez que escolheu as configurações de privacidade para um determinado serviço, esta configuração pode ser utiliza em outro.

Por isso, André configurou em seu navegador suas preferências quanto aos seus dados pessoais. Portanto, quando André acessa um determinado *website* que possua política de privacidade disponível no protocolo Platform for Privacy Preferences Project (P3P), automaticamente as configurações de privacidade são comparadas com as políticas do *website*.

Entretanto, ao acessar o *website* de compras online, André notou que suas configurações não puderam ser comparadas e que ele deveria fazê-lo de modo manual. Sendo assim, André gostaria que o *e-commerce* implementasse o protocolo P3P para fornecer as políticas de privacidade no formato adequado para verificar a compatibilidade com as preferências de privacidade do usuário. Para este cenário, o padrão de privacidade Platform for Privacy Preferences pode ser utilizado. A Figura 84 exibe a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero comparar automaticamente as configurações de privacidade.
Para que eu possa ter uma maior comodidade, visto que as políticas de privacidade são semelhantes em diversos serviços.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Preferências de Privacidade.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O website deve ter uma política de privacidade que possa ser traduzida em uma linguagem de marcação compatível com o P3P.
- O navegador do usuário deve suportar o P3P e estar configurado para enviar solicitações de P3P ao website.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Platform for Privacy Preferences.</td></tr>
</table>

Figura 84. História de Usuário Utilizando o Padrão de Privacidade Platform for Privacy Preferences.

Policy Matching Display

Luana definiu previamente em seu *smartphone* as suas preferências de privacidade. Atualmente ela está fazendo uso de um aplicativo financeiro e gostaria verificar se a política de privacidade deste está em conformidade com suas preferências.

Para isto, Luana gostaria que o aplicativo exibisse uma comparação entre os termos de uso da política de privacidade e as preferências de privacidade previamente definidas por ela em seu *smartphone*. Neste contexto, o padrão de privacidade Policy Matching Display pode ser aplicado. A Figura 85 descreve a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário. **Eu quero** verificar se minhas preferências de privacidade estão em conformidade com a política de privacidade do aplicativo. **Para que** eu possa gerenciar como meus dados são coletados, processados, armazenados e excluídos.		
Dados Pessoais: - Nome Completo. - E-mail. - Preferências de Privacidade.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Obter as preferências de privacidade do usuário para compará-las com a política de privacidade do aplicativo. - Fornecer feedback ao usuário sobre como as preferências de privacidade dele afetam a sua experiência com no aplicativo. - Para as preferências de usuário que não estão sendo atendidas pelo aplicativo, deve ser fornecido uma explicação detalhada do que se trata e permitir ao usuário alterar sua escolha.		
Recomendações de Padrões de Privacidade: - Policy Matching Display.		

Figura 85. História de Usuário Utilizando o Padrão de Privacidade Policy Matching Display.

Privacy-Aware Network Client

Leandro é gerente de uma empresa e precisa acessar de maneira remota o sistema de gestão empresarial para monitorar o desempenho de vendas e acompanhar dados financeiros. Porém, tanto os dados pessoais de Leandro quanto as informações confidenciais da empresa, devem ser protegidos contra violões de privacidade.

O padrão Privacy-Aware Network Client pode ser utilizado neste caso, pois visa estabelecer um *proxy* que analisa e interpreta as políticas de privacidade do servidor para fornecer resumos padronizados aos usuários. O usuário, por sua vez, só terá acesso ao servidor mediante aprovação à política recebida, enquanto isto não ocorrer, o usuário só poderá se comunicar com o servidor *proxy*. A Figura 86 aborda a história de usuário para o exemplo citado.

História de Usuário		
Como um gerente. **Eu quero** acessar o sistema de gestão empresarial remotamente. **Para que** eu possa monitorar o desempenho das vendas e acompanhar as transações financeiras.		
Dados Pessoais: - Nome Completo. - E-mail.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		

Restrições: - Não permitir o acesso não autorizado de terceiros ao servidor. - O gerente só poderá acessar o servidor mediante consentimento dos termos da política de privacidade. - Uma vez autorizada, a conexão deve ocorrer de modo criptografado para garantir a proteção dos dados do usuário e da empresa.
Recomendações de Padrões de Privacidade: - Privacy-Aware Network Client.

Figura 86. História de Usuário Utilizando o Padrão de Privacidade Privacy-Aware Network Client.

Increasing Awareness of Information Aggregation

Renata faz uso de uma plataforma de *streaming* de vídeo e notou que sua experiência com o uso do aplicativo está melhorando de acordo com suas preferências e histórico de visualizações. Entretanto, Renata gostaria de compreender quais dados pessoais a plataforma está coletando, como e com que finalidade, além de possibilitar ajustar suas preferências de privacidade.

Uma maneira de fornecer os detalhes almejados por Renata é pela implementação do padrão de privacidade Increasing Awareness of Information Aggregation, que possibilitará a Renata habilitar a opção de receber detalhes sobre a coleta, uso e compartilhamentos dos seus dados pessoais. A Figura 87 destaca a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** receber informações mais detalhadas sobre como minha atividade é rastreada e como as informações são utilizadas para me recomendar conteúdo. **Para que** me sinta mais confiante em usar a plataforma de streaming de vídeo.		
Dados Pessoais: - Nome Completo. - Data de Nascimento. - Preferências. - Recomendações. - Histórico de visualizações.	**Dados Pessoais Sensíveis:** - Nacionalidade.	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Possibilitar ao usuário habilitar a opção para receber detalhes da coleta, uso e armazenamento de seus dados pessoais. - Fornecer ao usuário informações detalhadas sobre como a atividade dele é rastreada na plataforma.		
Recomendações de Padrões de Privacidade: - Increasing Awareness of Information Aggregation.		

Figura 87. História de Usuário Utilizando o Padrão de Privacidade Increasing Awareness of Information Aggregation.

Informed Credential Selection

Tiago instalou um novo aplicativo financeiro para gerenciar sua conta bancária. Ao abrir o aplicativo pela primeira vez, ele deve realizar um cadastro no aplicativo informando seus dados pessoais, bancários, além de criar dados de autenticação, que pode ser realizada por diversas maneiras: cpf + senha, cpf + foto da face, cpf + datilograma, confirmação por mensagens de texto, entre outros.

Preocupado com a coleta de seus dados pessoais, Tiago gostaria de compreender detalhadamente todas as opções disponíveis e quais são os impactos em sua privacidade cada uma oferece. Para este cenário, o padrão de privacidade Informed Credential Selection pode ser utilizado. A Figura 88 exibe a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero selecionar minhas credenciais de login de forma informada.
Para que eu garanta a segurança da minha conta.</td></tr>
<tr><td>Dados Pessoais:
- CPF.
- Datilograma.
- Telefone.</td><td>Dados Pessoais Sensíveis:
- Imagem da Face.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- A plataforma deve exibir as opções de credenciais de login disponíveis (por exemplo, CPF + senha, login com biometria).
- Ao selecionar uma opção de credencial, a plataforma deve fornecer informações claras sobre os prós e contras de cada uma (por exemplo, nível de segurança, facilidade de uso).
- O usuário deve ser capaz de selecionar e alterar suas credenciais de login a qualquer momento.
- A plataforma deve garantir que as credenciais selecionadas sejam armazenadas de forma segura e criptografada.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Informed Credential Selection.</td></tr>
</table>

Figura 88. História de Usuário Utilizando o Padrão de Privacidade Informed Credential Selection.

Informed Secure Passwords

Jorge gostaria de criar uma nova conta em uma rede social. As informações pessoais necessárias são: nome completo, E-mail, data de nascimento, gênero e senha. Preocupado com a privacidade e segurança de sua conta, Jorge gostaria de

protegê-la com uma senha segura, porém está em dúvida qual o tamanho ela deve conter e quais caracteres utilizar em sua composição.

O padrão de privacidade Informed Secure Passwords pode ser utilizado neste caso, pois auxilia os usuários na criação de senhas seguras, sugerindo um número mínimo de caracteres, uso de caracteres especiais, numéricos, além de dar *feedback* em tempo real do quão complexa a senha está. A Figura 89 aborda a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um novo usuário.
Eu quero criar uma senha segura.
Para que proteger e acessar minha conta.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Data de Nascimento.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O sistema deve exigir que a senha tenha pelo menos 8 caracteres, incluindo pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.
- Ao criar uma senha, o usuário deve receber feedback em tempo real sobre a força da senha, incluindo a contagem de caracteres e a combinação de caracteres especiais, letras maiúsculas e minúsculas e números.
- O sistema deve permitir que o usuário saiba se sua senha é fraca e oferecer sugestões para melhorá-la.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Informed Secure Passwords.</td></tr>
</table>

Figura 89. História de Usuário Utilizando o Padrão de Privacidade Informed Secure Passwords.

Unusual Activities

Diego possui cadastro em uma loja virtual. Recentemente ele foi surpreendido com E-mails de confirmação de compras que ele não havia realizado. Ao investigar, verificou que sua conta tinha sido hackeada por criminosos que conseguiram fazer compras em seu nome.

Após conseguir entrar em contato com a loja virtual e recuperar a senha de sua conta, Diego gostaria que a plataforma, ao identificar atividades incomuns e suspeitas, enviassem E-mails de alerta aos usuários notificando-os do ocorrido. Desta maneira, medidas poderiam ser tomadas antes que alterações e compras realizadas por pessoas mal-intencionadas fossem concretizadas, conforme estabelece o padrão de

privacidade Unusual Activities. A Figura 90 apresenta a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero receber E-mails me informando de atividades incomuns em minha conta.
Para que eu possa tomar medidas imediatas para proteger minhas informações pessoais.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Geolocalização.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- O sistema deve monitorar os usuários ao realizarem login na plataforma.
- Ao constatar uma atividade incomum, um e-mail de alerta deve ser enviado ao usuário.
- Enquanto o usuário não confirmar a identidade, o acesso deve ficar suspenso.
- Fornecer ao usuário um histórico de atividades em sua conta para que possa ser revisado por ele com o intuito de verificar atividades suspeitas e não autorizadas.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Unusual Activities.</td></tr>
</table>

Figura 90. História de Usuário Utilizando o Padrão de Privacidade Unusual Activities.

Informed Implicit Consent

Daniela instalou um aplicativo de edição de imagem. Durante o processo de registro, o aplicativo solicitou que ela permitisse o acesso à sua localização, informações de contato e fotos, sem explicar claramente como esses dados seriam utilizados. Daniela não se sentiu confortável em compartilhar os dados exigidos e gostaria que o aplicativo apresentasse de forma clara os termos de uso para que, assim, fornecesse o consentimento quanto ao uso de seus dados pessoais.

Além disso, Daniela gostaria que a plataforma disponha de controles de privacidade eficazes os quais permitam que ela controle o acesso e uso de suas informações pessoais e, se necessário, revogar o consentimento a qualquer momento, conforme menciona o padrão de privacidade Informed Implicit Consent. A Figura 91 aborda a história de usuário para o cenário especificado.

História de Usuário		
Como um usuário. **Eu quero** receber informações claras e simples sobre como os dados pessoais serão coletados, usados e compartilhados com terceiros. **Para que** eu possa decidir em consentir com a coleta, uso e armazenamento dos meus dados pessoais.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - O aplicativo deve fornecer informações claras e simples sobre como os dados do usuário serão coletados, usados e compartilhados com terceiros. - O usuário deve ser capaz de entender facilmente como seus dados serão usados e ter a opção de consentir ou não com a coleta de dados. - O aplicativo deve fornecer opções para que o usuário gerencie suas preferências de privacidade e possa revogar o consentimento a qualquer momento.		
Recomendações de Padrões de Privacidade: - Informed Implicit Consent.		

Figura 91. História de Usuário Utilizando o Padrão de Privacidade Informed Implicit Consent.

Minimal Information Asymmetry

Raquel instalou um aplicativo de *delivery* de alimentos. Ao acessar o aplicativo, foi solicitado que ela informasse algumas informações pessoais, como nome completo, data de nascimento, gênero, e-mail, endereço, entre outras. Raquel ficou um pouco desconfortável ao fornecer essas informações, pois, em sua concepção, são dados desnecessários para o objetivo final do aplicativo.

Raquel gostaria que o aplicativo solicitasse apenas informações mínimas necessárias para que ela consiga fazer o seu pedido e recebê-lo em sua residência. Para isso, o padrão de privacidade Minimal Information Asymmetry pode ser utilizado. A Figura 92 destaca a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** fazer um pedido de alimento sem compartilhar mais informações pessoais do que o necessário. **Para que** eu possa minimizar os riscos de má utilização ou roubo de informação por terceiros.		
Dados Pessoais: - Nome Completo. - Endereço.	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:** 5 anos.
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		

Restrições: - O compartilhamento dos dados pessoais do usuário só poderá ser realizado mediante consentimento. - Deve ser solicitado apenas as informações essenciais para a finalidade do aplicativo. - Oferecer ao usuário a opção de revisar e editar as informações que foram informadas antes de confirmar o pedido. - Oferecer ao usuário informações claras e objetivas sobre como os dados pessoais serão utilizados e protegidos.
Recomendações de Padrões de Privacidade: - Minimal Information Asymmetry.

Figura 92. História de Usuário Utilizando o Padrão de Privacidade Minimal Information Asymmetry.

Personal Data Table

Nicolas utiliza um aplicativo financeiro para realizar suas transações bancárias. Sabendo a importância de manter a privacidade de seus dados pessoais, Nicolas acessa a política de privacidade do aplicativo para obter informações de quais dados o aplicativo coleta, como armazena e processa e com quem compartilha.

Porém, Nicolas gostaria de obter essas informações de modo mais direto e rápido, sem precisar ler na íntegra o documento da política de privacidade. Um modo de possibilitar aos usuários acompanhar informações de privacidade de seus dados pessoais é a utilização do padrão de privacidade Personal Data Table, que visa resumir em formato de tabela todos os dados pessoais coletados pelo aplicativo. A tabela deve mostrar o tipo de dados coletados, a finalidade da coleta, o período de retenção e a possibilidade de excluir ou modificar esses dados. A Figura 93 exibe a história de usuário para o contexto mencionado.

História de Usuário		
Como um usuário. **Eu quero** poder visualizar todos os meus dados pessoais coletados pelo aplicativo em uma tabela clara e organizada. **Para que** eu possa compreender quais dados o aplicativo possui sobre mim e ter controle sobre eles.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Permitir ao usuário visualizar todos os dados pessoais coletados pelo aplicativo em uma tabela organizada. - A tabela deve exibir o tipo de dado coletado, finalidade da coleta, o período de retenção e a possibilidade de excluir ou modificar esses dados. - Permitir ao usuário acessar o documento de política de privacidade na íntegra.		
Recomendações de Padrões de Privacidade: - Personal Data Table.		

Figura 93. História de Usuário Utilizando o Padrão de Privacidade Personal Data Table.

Preventing Mistakes or Reducing Their Impact

Amanda utiliza um serviço de armazenamento e sincronização de arquivos para fazer *backups* na nuvem. Eventualmente Amanda compartilha seus arquivos com amigos, familiares e colegas de trabalho. Porém, Amanda tem receio que, por um erro dela, compartilhe arquivos pessoais com pessoas que não deveriam ter acesso.

Por este motivo, Amanda gostaria que o serviço de armazenamento implementasse o padrão de privacidade Preventing Mistakes or Reducing Their Impact, para que, ao alterar o nível de visibilidade de um determinado arquivo, alertas fossem exibidos fornecendo dados como: nome do arquivo, tamanho, nível de visualização, terceiros que terão acesso, entre outros. O arquivo só poderia ser compartilhado mediante a confirmação de Amanda, minimizando as chances do compartilhamento ocorrer por engano. A Figura 94 destaca a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero compartilhar arquivos com pessoas específicas.
Para que elas acessem, manipulem e realizem download dos arquivos disponíveis.</td></tr>
<tr><td>Dados Pessoais:
- Nome completo.
- E-mail.
- Arquivos pessoais compartilhados.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Permitir ao usuário selecionar um ou mais arquivos para compartilhar com terceiros.
- O sistema deve exibir uma lista com todos os arquivos que serão compartilhados, além dos nomes e E-mails das pessoas que terão acesso às informações.
- O compartilhamento só ocorrerá mediante a confirmação do titular de dados.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Preventing Mistakes or Reducing Their Impact.</td></tr>
</table>

Figura 94. História de Usuário Utilizando o Padrão de Privacidade Preventing Mistakes or Reducing Their Impact.

Privacy Awareness Panel

Jaqueline possui um perfil em uma rede social e está preocupada com sua privacidade de dados, pois não compreende como suas informações pessoais são

coletadas e utilizadas pela plataforma. Ela gostaria de acessar os detalhes da política de privacidade da rede social de maneira objetiva e amigável.

Para isto, o padrão de privacidade Privacy Awareness Panel pode ser implementado, pois visa conscientizar os titulares de dados por meio de um painel de configurações de privacidade que exibe quais informações pessoais são coletadas, como são processadas e armazenadas e com quem são compartilhadas. A Figura 95 descreve a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero obter informações objetivas e de fácil compreensão de como meus dados pessoais estão sendo tratados.
Para que eu possa revisar minhas preferências de privacidade e ter a garantia eu meus dados pessoais estão protegidos.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Exibir em um painel de configuração de privacidade todas as informações sobre a coleta, processamento, armazenamento e compartilhamento de dados pessoais do usuário.
- Permitir ao usuário alterar suas configurações de privacidade.
- O painel de configurações de privacidade deve ser facilmente encontrado e acessado pelo usuário.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Awareness Panel.</td></tr>
</table>

Figura 95. História de Usuário Utilizando o Padrão de Privacidade Privacy Awareness Panel.

Privacy Dashboard

Flávio é usuário de um aplicativo de *delivery* de refeições. Para o uso do aplicativo, Flávio compreende que seus dados pessoais são coletados, como por exemplo, nome completo, E-mail, telefone, endereço, histórico de pedidos, preferências de comidas, informações de pagamento, entre outros. Porém, Flávio gostaria que o aplicativo exibisse a ele um painel contendo as informações pessoais que foram coletadas no decorrer dos meses, oferecendo uma maior transparência e confiança para com os usuários.

Além disso, o sistema deveria permitir aos usuários controlar suas configurações de privacidade, como optar pelo não recebimento de E-mails promocionais e limpeza do histórico de pesquisas e pedidos. Neste contexto, o padrão de privacidade Privacy Dashboard pode ser utilizado. A Figura 96 destaca a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero obter um relatório dos dados pessoais que foram coletados pelo aplicativo.
Para que eu possa revisar, gerenciar e tomar decisões informadas sobre a minha privacidade.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Exibir de maneira detalhada em uma lista os dados pessoais coletados do usuário.
- Exibir uma lista de terceiros com quem os dados pessoais do usuário são compartilhados.
- Permitir ao usuário visualizar e gerenciar o compartilhamento de suas informações pessoais.
- Permitir ao usuário revogar o acesso do aplicativo a determinadas informações pessoais.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Dashboard.</td></tr>
</table>

Figura 96. História de Usuário Utilizando o Padrão de Privacidade Privacy Dashboard.

Privacy Color Coding

Daiane decidiu revisar as configurações de privacidade do seu perfil em uma rede social. Ao acessar o painel de configuração de privacidade, ela se deparou com uma extensa lista de tópicos que são configurados, cada um com seu nível de visibilidade, como por exemplo, foto de perfil: público, publicações: apenas a amigos, E-mail: apenas ao titular de dados, entre outros.

Daiane gostaria que a opções de visibilidade fossem relacionadas a cores, facilitando a visualização dos tópicos das configurações de privacidade. Por exemplo, tópicos que possuem acesso público poderiam ser identificados pela cor vermelha, tópicos visíveis apenas a amigos, amarela, e tópico visíveis a apenas ao titular de dados, verde. Neste cenário, pode-se aplicar o padrão de privacidade Privacy Color Coding. A Figura 97 apresenta a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero configurar minhas opções de privacidade de maneira intuitiva e amigável.
Para que eu possa manter meus dados pessoais seguros e protegidos de acessos a pessoas não autorizadas.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Definir, de maneira coerente, as cores que representam cada nível de visibilidade para que não cause confusão ou erros de interpretações.
- As representações de forma visual devem ser complementadas por descrições textuais para que a informação seja compreensível a todos os usuários.
- Permitir ao usuário personalizar a escolha das cores ou utilizar as cores padrão.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Privacy Color Coding.</td></tr>
</table>

Figura 97. História de Usuário Utilizando o Padrão de Privacidade Privacy Color Coding.

Privacy Mirrors

Alexandre trabalha no almoxarifado de uma organização. Para facilitar as requisições de compras, ele elaborou formulários que devem ser preenchidos pelos demais colaboradores. Estes formulários ficam disponíveis em uma pasta compartilhada no sistema de armazenamento na nuvem da própria instituição a qual todos os colaboradores da organização possuem acesso.

Porém, Alexandre notou que os colaboradores estavam modificando os documentos originais disponibilizado por ele. Para resolver este problema, o padrão Privacy Mirrors pode ser aplicado, pois o sistema criará uma cópia espelhada da pasta compartilhada para cada colaborador. Sendo assim, cada usuário possuirá acesso apenas a própria cópia espelhada da pasta e não a pasta original, o que o impediria de editar os arquivos disponibilizados por Alexandre. A Figura 98 destaca a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero que os arquivos compartilhados por mim sejam espelhados em pastas pessoais de outros usuários.
Para que os demais usuários tenham controle e privacidade sobre seus próprios arquivos e informações.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Arquivos compartilhados.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
</table>

Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
Restrições: - O compartilhamento só poderá ocorrer mediante o consentimento informado pelo titular dos dados. - Permitir ao usuário compartilhar com usuários específicos. - Permitir ao usuário visualizar os detalhes de cada arquivo, bem como os nomes dos usuários que estejam espelhando o arquivo selecionado. - Permitir ao usuário revogar o compartilhamento de um arquivo com os demais usuários.
Recomendações de Padrões de Privacidade: - Privacy Mirrors.

Figura 98. História de Usuário Utilizando o Padrão de Privacidade Privacy Mirrors.

Trust Evaluation of Services Sides

Luiza está pesquisando um determinado produto para compra-lo e o encontrou em uma loja virtual a qual nunca realizou nenhuma transação. Com receio de fornecer seus dados pessoais na plataforma, Luiza gostaria de verificar a avaliação do *website* antes de realizar a compra. Neste caso, o padrão Trust Evaluation of Services Sides pode ser aplicado para fornecer ao usuário informações detalhadas sobre a segurança e confiabilidade do site, incluindo avaliações de outros usuários, informações sobre as práticas de segurança adotadas pelo site e a verificação de certificados de segurança. A Figura 99 descreve a história de usuário para o exemplo citado.

História de Usuário		
Como um usuário. **Eu quero** avaliar a segurança e confiabilidade do site antes de inserir meus dados pessoais e informações de pagamento. **Para que** eu possa me certificar que o website é confiável e protegerá minhas informações pessoais.		
Dados Pessoais:	**Dados Pessoais Sensíveis:**	**Tempo de Retenção:**
Leis e Regulamentos: - Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).		
Restrições: - Exibir ao usuário as avaliações anteriores realizadas por usuários que realizaram transações com o website. - Fornecer informações claras e detalhadas sobre as práticas de segurança adotadas pelo website, como uso de criptografia e proteção de dados. - Exibir ao usuário os certificados de segurança utilizados pelo website. - Permitir que o usuário avalie a confiabilidade e segurança do website após a conclusão da transação e compartilhe sua experiência com outros usuários.		
Recomendações de Padrões de Privacidade: - Trust Evaluation of Services Sides.		

Figura 99. História de Usuário Utilizando o Padrão de Privacidade Trust Evaluation of Services Sides.

Who’s Listening

Rogério trabalha no time de *marketing* em uma organização e utiliza uma plataforma colaborativa para criarem as artes que serão utilizadas na comunicação, distribuição, precificação e formatação dos produtos e serviços das empresas.

A plataforma utilizada pelo time de *marketing* permite edições simultâneas no mesmo documento, entretanto, não há como identificar em tempo real quantos usuários estão acessando e editando o documento, prejudicando a comunicação entre os colaboradores e a segurança dos dados pessoais e empresarias.

A fim de melhorar a transparência sobre o compartilhamento de dados, Rogério gostaria que a plataforma exibisse quais são os colaboradores que possuem acesso a determinados documentos e quais são seus privilégios. Além disso, quando um colaborador estiver acessando e/ou modificando um documento, os demais usuários deverão ser notificados. Neste contexto, o padrão Who’s Listening pode ser implementado. A Figura 100 exibe a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um colaborador.
Eu quero ser notificado quando outro colaborador acessar ou editar algum documento compartilhado.
Para que eu possa monitorar o acesso aos documentos compartilhados de forma eficiente.</td></tr>
<tr><td>Dados Pessoais:</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Exibir uma notificação a todos os colaboradores envolvidos quando ocorre um novo acesso ao documento.
- Exibir, em tempo real, quais modificações cada colaborador está realizando.
- Permitir a cada colaborador configurar suas preferências de privacidade.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Who’s Listening.</td></tr>
</table>

Figura 100. História de Usuário Utilizando o Padrão de Privacidade Who’s Listening.

Federated Privacy Impact Assessment

Priscila gostaria de realizar cotações de seguro para seu automóvel. Para isto, baixou o aplicativo de uma das seguradoras e inseriu seus dados pessoais a fim de obter um orçamento para seu perfil. Ela notou que a seguradora possuía informações de outras seguradoras, como histórico de sinistros ocorrido no passado.

Ao investigar, Priscila notou que as empresas de seguros possuem uma rede federada em que compartilham dados de seus clientes uma com as outras, o que a deixou preocupada, pois há várias possíveis ameaças e riscos à sua privacidade que podem surgir, como por exemplo, violações, acesso não autorizado, uso indevido, entre outras.

Para este cenário, pode-se utilizar o padrão de privacidade Federated Privacy Impact Assessment, que visa realizar uma avaliação de impacto de privacidade para identificar e gerenciar os riscos decorrentes do compartilhamento de informações pessoais entre sistemas em uma rede federada. A Figura 101 destaca a história de usuário para o contexto mencionado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero realizar cotação de seguros para meu veículo.
Para que eu possa comparar diferentes opções de cobertura e escolher a melhor para meu perfil.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.
- Endereço.
- Telefone.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Exibir de maneira clara de objetiva qual é o propósito da coleta de dados pessoais.
- Exibir ao usuário como é realizado a coleta, processamento, uso, armazenamento e compartilhamento das informações pessoais dos titulares de dados.
- Possibilitar ao usuário acessar e corrigir seus dados pessoais mantidos pela empresa.
- O compartilhamento dos dados pessoais com terceiros só poderá ser realizado mediante a obtenção do consentimento informado pelo titular dos dados.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Federated Privacy Impact Assessment.</td></tr>
</table>

Figura 101. História de Usuário Utilizando o Padrão de Privacidade Federated Privacy Impact Assessment.

Obligation Management

Augusto tem preferência por realizar compras em lojas virtuais a lojas físicas pela comodidade em receber seus produtos em sua residência, sem precisar sair de casa. Porém, notou que a loja virtual a qual ele realiza suas compras terceiriza a entrega do produto à uma empresa de transportes. Para que seu produto seja

entregue corretamente em seu endereço, alguns dados pessoais dos usuários são compartilhados entre ambas as empresas, o que deixou Augusto receoso em relação a seus dados pessoais.

Ele gostaria de garantir que as empresas envolvidas estejam cumprindo com suas obrigações legais em relação à proteção dos dados pessoais dos clientes. Para este exemplo, o padrão Obligation Management pode ser utilizado, garantindo que apenas informações necessárias para a entrega do produto sejam compartilhadas e mantidas de maneira segura e confidencial pela empresa de transportes, além de permitir o acesso, edição e exclusão dos dados pelo titular. A Figura 102 exibe a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero que a companhia cumpra suas obrigações legais quanto à proteção dos meus dados pessoais.
Para que minhas informações permaneçam seguras e confidenciais, mesmo quando compartilhadas com empresas terceiras.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Endereço.
- Telefone.</td><td>Dados Pessoais Sensíveis:</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Coletar apenas informações necessárias para a entrega do produto.
- A empresa terceira deve comprovar que possui políticas de privacidade bem definidas e que mantém as informações pessoais seguras e confidenciais.
- O compartilhamento com terceiros só pode ocorrer mediante a obtenção do consentimento explícito do titular dos dados.
- Permitir ao titular dos dados acessar, editar ou excluir suas informações pessoais a qualquer momento.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Obligation Management.</td></tr>
</table>

Figura 102. História de Usuário Utilizando o Padrão de Privacidade Obligation Management.

Sticky Policies

Isabela se matriculou em um curso de línguas estrangeiras. Para que ela tenha acesso ao material didático, bem como acompanhar sua agenda de estudos e seus dados de pagamento, ela foi informada que é necessário fazer download e cadastro no aplicativo oficial da escola.

Ao ler a política de privacidade do aplicativo, ela verificou-se que o relacionamento com o cliente e pagamento são realizados por empresas terceiras.

Com isso, Isabela ficou apreensiva, pois para um melhor relacionamento com os alunos, a empresa terceira deve ter acesso aos dados pessoais dos estudantes.

Neste cenário, Isabela gostaria que a plataforma comunicasse claramente aos seus usuários como os dados pessoais são utilizados e quem possui acesso, além de possibilitar aos usuários configurar quais dados podem ser compartilhados com terceiros e quais devem permanecer privados.

Para garantir a privacidade e controle das informações pessoais dos usuários no aplicativo, o padrão de privacidade Sticky Policies pode ser utilizado. A Figura 103 descreve a história de usuário para o cenário especificado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ter controle sobre quem pode acessar minhas informações pessoais e como são utilizadas.
Para que minhas informações pessoais não sejam compartilhadas com terceiros sem minha autorização.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- E-mail.
- Data de Nascimento.
- Telefone.
- Histórico de aulas.
- Desempenho.
- Informações de Pagamento.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 5.172 - Sistema Tributário Nacional.</td></tr>
<tr><td colspan="3">Restrições:
- Os dados pessoais do usuário só poderão ser compartilhados com terceiros mediante o consentimento explícito do mesmo.
- O compartilhamento de dados só poderá ocorrer mediante a um propósito específico.
- Fornecer ao titular dos dados informações de quais dados pessoais estão sendo compartilhados e com quem.
- Fornecer ao usuário mecanismos para que, se ele julgar necessário, possa excluir seus dados pessoais ou restringir o compartilhamento com terceiros a qualquer momento.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Sticky Policies.</td></tr>
</table>

Figura 103. História de Usuário Utilizando o Padrão de Privacidade Sticky Policies.

Identity Federation Do Not Track Pattern

Melissa possui uma conta de um provedor de e-mails. Recentemente, ela foi realizar um cadastro em uma rede social e verificou que poderia utilizar suas informações pessoais, como login e senha, do próprio provedor de e-mail que já

possuía cadastro. Receosa como uma empresa possui seus dados pessoais sem sua autorização, ela gostaria de limitar o uso de suas credenciais para outros serviços.

Neste cenário, Melissa gostaria que o provedor de e-mail possibilite aos seus usuários optar por compartilhar ou não suas informações pessoais com sites de terceiros, mesmo que sejam empresas que usam o mesmo sistema de login federado. Para este caso, o padrão de privacidade Identity Federation Do Not Track Pattern pode ser utilizado. A Figura 104 aborda a história de usuário para o exemplo citado.

<table>
<tr><td colspan="3">História de Usuário
Como um usuário.
Eu quero ter a opção de não compartilhar minhas informações com outros sites de terceiros.
Para que eu possa controlar melhor minha privacidade.</td></tr>
<tr><td>Dados Pessoais:
- Nome Completo.
- Data de Nascimento.
- E-mail.
- Senha.</td><td>Dados Pessoais Sensíveis:
- Gênero.</td><td>Tempo de Retenção:
5 anos.</td></tr>
<tr><td colspan="3">Leis e Regulamentos:
- Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD).</td></tr>
<tr><td colspan="3">Restrições:
- Fornecer ao usuário a possibilidade de ativar ou não a opção de compartilhar informações de login com empresas terceiras.
- Garantir que empresas terceiras não coletarão informações pessoais dos usuários para outros fins que não seja o de realizar login em suas respectivas plataformas.
- Apenas dados necessários para a realização do login devem ser compartilhados.
- Fornecer ao usuário informações de quais dados pessoais estão sendo compartilhados, com que empresa e para que fim.</td></tr>
<tr><td colspan="3">Recomendações de Padrões de Privacidade:
- Identity Federation Do Not Track Pattern.</td></tr>
</table>

Figura 104. História de Usuário Utilizando o Padrão de Privacidade Identity Federation Do Not Track Pattern.

APÊNDICE H – QUESTIONÁRIO DE AVALIAÇÃO (TAM)

1. De acordo com sua percepção da Facilidade de Uso do Processo, Papel e Artefatos propostos, o quanto você concorda com as seguintes afirmações:

Afirmações	Discordo Totalmente	Discordo Parcialmente	Não Discordo e Não Concordo	Concordo Parcialmente	Concordo Totalmente
E1. O processo proposto é compreensível.	-	-	-	-	-
Justifique sua resposta:					
E2. Os artefatos (i) Mapeamento dos Padrões de Privacidade e Princípios do *Privacy by Design* e (ii) Repositório de Histórias de Usuário são compreensíveis.	-	-	-	-	-
Justifique sua resposta:					
E3. As responsabilidades do Guardião de Privacidade são compreensíveis.	-	-	-	-	-
Justifique sua resposta:					
E4. Acho fácil incluir o processo proposto no processo de desenvolvimento que é utilizado atualmente na organização.	-	-	-	-	-
Justifique sua resposta:					

2. De acordo com sua percepção da Utilidade do Processo Proposto, o quanto você concorda com as seguintes afirmações:

Afirmações	Discordo Totalmente	Discordo Parcialmente	Não Discordo e Não Concordo	Concordo Parcialmente	Concordo Totalmente
U1. A utilização do processo fará com que os requisitos de privacidade de dados pessoais sejam considerados desde o início do processo de desenvolvimento de software.	-	-	-	-	-
Justifique sua resposta:					
U2. A utilização do processo evitará o retrabalho da aplicação de requisitos de privacidade de dados pessoais do time de desenvolvimento de software.	-	-	-	-	-
Justifique sua resposta:					
U3. Eu considero o processo útil para implementar requisitos de privacidade de dados pessoais.	-	-	-	-	-
Justifique sua resposta:					
U4. Eu recomendaria o processo de privacidade para engenheiros de software.	-	-	-	-	-
Justifique sua resposta:					

3. De acordo com sua possível Intenção de Uso Futuro do Processo Proposto, o quanto você concorda com a seguinte afirmação:

Afirmações	Discordo Totalmente	Discordo Parcialmente	Não Discordo e Não Concordo	Concordo Parcialmente	Concordo Totalmente
I1. Eu utilizaria o processo proposto no desenvolvimento de software da organização.	-	-	-	-	-
Justifique sua resposta:					